Pricing and Hedging Cybercrime News[*]

Jiatao Liu[†] Ian W. Marsh[‡] Yajun Xiao[§]

April 9, 2024

Abstract

Stocks exhibiting positive sensitivity to cybercrime risk—a positive beta with respect to a cybercrime news narrative measure—command lower subsequent returns, implying a negative risk premium for assets that offer hedging during cybercrime surges. Our long-short portfolio strategy confirms the value of such stocks in mitigating cybercrime exposure across 112 significant cyber incidents. We pinpoint determinants of firms' cybercrime betas, identifying human capital investment in corporate governance, minimal industry-wide cybercrime entanglements, limited digital activities, and less data-centric business focus. Our asset pricing results provide a reference point for cyber insurance pricing and suggest huge potential growth in insurance coverage.

JEL Classification: G11, G12, C13, E20

Keywords: Cybercrime risk, hedging, corporate governance, industry peers, digitization, IT investment

[*] Previously circulated as "Cybercrime News and Hedging in the ICAPM Framework". We are grateful to Jack Bao, Hui Chen, Liang Fu, Xuezhong (Tony) He, Shiyang Huang, Aneel Keswani, Kai Li (PHBS), Junye Li, Shen Lin (discussant), Yunting Liu, Yang Liu (discussant), Xiaomeng Lu, Jun Pan, Richard Payne, Maik Schmeling, Paolo Volpin, Ke Wu (discussant), Xiao Xiao, Yapei Zhang, Shen Zhao (discussant), Xiaofei Zhao (discussant) and participants in CFAM 2023, CFRN Tsinghua University, CICF 2023, CES 2023 North America Conference, FMA European 2023, Hunan University, TJU Finance Workshop, University of Bologna, and XJTLU Asset Pricing Workshop for discussions and helpful comments. We gratefully acknowledge the London Stock Exchange Group (LSEG) and MarketPsych Data for providing the news data, and Spicework's Ziff Davis for providing the IT investment data for our research. We thank Kenneth R. French, Lu Zhang, Gerard Hoberg and Gordon Phillips for providing an open access for their data library. We thank Chengqi Duan, Runchen Ji, Jinlu Xue, and Yiheng Yao for their research assistance. All errors are our own.

[†] Department of Finance, Xi'an Jiaotong-Liverpool University; Email: `Jiatao.Liu@xjtlu.edu.cn`

[‡] Bayes Business School, City, University of London; Email: `i.marsh@city.ac.uk`

[§] Department of Finance, Xi'an Jiaotong-Liverpool University; Email: `Yajun.Xiao@xjtlu.edu.cn`

1 Introduction

As the financial landscape reckons with the burgeoning risks of cybersecurity and environmental concerns, our understanding of market dynamics undergoes a pivotal shift. Research by Choi et al. (2020), Krueger et al. (2020), Engle et al. (2020), Bolton and Kacperczyk (2021), and Hsu et al. (2022) on climate risk underscores a broader recognition of evolving risks that reshape market valuations and hedging strategies. Mirroring this evolution, cybersecurity, with a particular focus on cybercrime, has surfaced as a significant economic challenge as documented by the U.S. Council of Economic Advisers and the Center for Strategic and International Studies.[1] In this context, contributions by Kamiya et al. (2021), Eisenbach et al. (2022), Florackis et al. (2023), Jamilov et al. (2023), and Jiang et al. (2024) have been crucial in elevating the discourse on cybersecurity risk, placing it alongside climate risk as a key emergent factor in financial markets.

Building on these foundations, our paper aims to bridge the gap between recognizing these evolving risks and devising practical hedging solutions. By introducing a cybercrime news shock measure derived from a high-frequency news dataset, we explore effective hedging portfolios that cater to the unique challenges posed by cyber threats. Furthermore, we delve into the determinants of cybercrime hedging mechanisms, identifying the attributes that fortify firms' defenses against cybercrime risks. This approach not only addresses the immediate need for risk management techniques but also contributes to a deeper understanding of how technological shifts are intricately linked to financial market resilience in the digital era.

To test the impact of cybercrime on the cross-section of expected stock returns we first construct a cybercrime news shock measure from a news dataset at the daily frequency, distributed as the Refinitiv MarketPsych Index of cybercrime. This is a score derived from articles published in media outlets including both news and social media. We then estimate monthly cybercrime betas using rolling regressions of daily excess returns on innovations in the Refinitiv cybercrime news index for U.S. stocks. Recognizing the issues arising from using sensitivities to a non-traded

[1] The U.S. Council of Economics Advisers has reported that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016 (CEA, 2018). The Center for Strategic and International Studies (2018) claims that almost 1% of global GDP, close to $600 billion, is lost to cybercrime each year.

economic series in asset pricing tests, we construct a cybercrime tracking portfolio. Portfolios formed on the basis of sensitivities to the tracking series show that stocks with positive sensitivity to the cybercrime tracking portfolio generate significantly lower next-month returns than those from negative sensitivity stocks. The high-minus-low (HL) portfolio generates a highly statistically significant average excess return of -0.95% per month, and survives controlling for many other factors. That is, stocks that offer positive returns when there are positive shocks to cybercrime command a high price and hence offer low expected returns. Stocks that vary negatively with cybercrime shocks, conversely, earn a positive risk premium. We show that the return differences are driven by cybercrime exposures rather than well-known stock characteristics or risk factors by examining conditional bivariate sorts using classical pricing characteristics and both firm and portfolio-level Fama-MacBeth regression tests.[2] Our contribution here is in simplifying the method used to estimate firm-level exposure to cybercrime compared with the literature that largely relies upon complex text analysis of 10-K filings or analyst conference call transcripts. In particular, our approach is easily generalizable to assets and jurisdictions where regulatory filings and earnings call transcripts are less reliable or even simply not available.

Our second contribution is to identify four distinct factors that lead firms to have different exposures to cybercrime news risk, particularly during times of higher cybercrime news coverage in the media. First, we demonstrate a positive relationship between cybercrime beta and corporate governance quality. Firms with fewer accruals and better governance scores – both relatively broad proxies for the quality of corporate governance – or that devote more board-level resources to risk management, informatics, and technology roles have higher cybercrime betas.

Second, we examine the influence of product market connections on firms' cybercrime risk exposure. Using a unique firm-level cybercrime news index together with firm peer groups defined using Hoberg and Phillips (2016)'s product market similarity measure, our study shows that firms

[2] We control for size and book-to-market (Fama and French, 1992;1993), profitability and investment (Fama and French, 2015; Hou et al., 2015), betas with the market factor, with market volatility (Ang et al., 2006; Campbell et al., 2018) and with economic policy uncertainty (Brogaard and Detzel, 2015), momentum (Jegadeesh and Titman, 1993), short-term reversal (Jegadeesh, 1990), illiquidity (Amihud, 2002), idiosyncratic volatility (Ang et al., 2006), and the dispersion of analyst earnings forecasts (Diether et al., 2002).

with more peers mentioned in recent cybercrime news stories are perceived as being more vulnerable to systemic cyber threats. The pervasive nature of cybercrime means that the negative effects of close competitors being attacked on a firm's perceived vulnerability outweigh any competitive advantages that the firm may have from seeing its competitors suffer from cybercrime.

Third, employing a text-based measure of firms' digitization, we explore the relation between firm digitization and cybercrime risk. The findings reveal a negative relation, indicating that less digitized firms may be perceived as safer investments during periods of heightened cybercrime concern. Our analysis contributes to the economic discourse by highlighting the need for firms to balance digital innovation with cybersecurity measures, enriching the literature on the economics of cybersecurity in the digital era.

Fourth, using a novel IT investment dataset, we explore the relationship between a firm's IT spending and its cybercrime beta, particularly during times of high cybercrime news coverage in the media. Following Brynjolfsson and McElheran (2016), we take IT investment scaled by assets as a proxy for the intensity of data-adoption practices in a firm. We show that firms that are positively exposed to cybercrime risk (i.e. have low cybercrime betas) tend to have high IT budgets and high IT/Assets ratios. Using the data innovation framework of Gomes et al. (2023), we argue that such companies are successfully adopting business models focused on the data economy such that their high IT spending translates into rapid growth. But this success also makes them both a specific target for cybercriminals and highly exposed to systematic problems caused by cybercrime. Conversely, high cybercrime beta firms have low IT/Assets ratios. They are less attractive to cyber criminals and less exposed to cyber risks. We show that in periods of heightened cybercrime news, the IT/Assets ratio negatively correlates with firms' cybercrime betas. At a finer level of granularity, higher-scaled spending on IT hardware, software, communications, and (but not services) is averse by investors when they are most sensitive to cybercrime.

Our third contribution is to examine the performance of a cybercrime hedging strategy based on cybercrime betas which we then use to inform discussions of the insurance cost of cybercrime risks. Using an event study approach, we show that across 112 major cybercrime incidents reported by the Center for Strategic and International Studies (CSIS), a strategy of taking a long position in high cybercrime beta stocks and a short position in low cybercrime beta stocks generates an average two-day post-event abnormal return of 0.37%. A back of the envelope calculation suggests that market-wide, this portfolio generates gains of around $86 billion per year, comparable to the $60-110 billion of annual losses to cyber crime estimated by the Council of Economic Advisors.

We then build upon our asset pricing tests and quantify an annualized ex-post cybercrime risk premium of 5.28% which we use to provide a reference price for cyber risk insurance. Based on another simple calculation, we demonstrate that the insurance industry could charge a market-implied risk premium of between $42.1 and $141.31 billion per year, depending on coverage. Given recent estimates that direct cybersecurity premiums total around just $3 billion, our figures reveal substantial room for increased coverage of cyber risks.

Related Literature Our paper is related to several strands of the literature. We directly contribute to a burgeoning literature that studies emerging and increasingly important risks such as climate risk (Andersson et al., 2016; Engle et al., 2020; Huynh and Xia, 2021) and cyber risk (Kamiya et al., 2021; Eisenbach et al., 2022; Florackis et al., 2023; Jamilov et al., 2023; Jiang et al., 2024) in the economy. With the rapid growth of information technology in the economy, our study focuses on the implications of the systematic risk from cybercrime. We add to this literature by showing that stocks that positively covary with innovations in cybercrime news have lower expected returns. To hedge against these unfavorable shifts, investors prefer holding stocks with higher covariance with cybercrime and accept lower expected returns.

In the specific field of cyber risk, studies by Florackis et al. (2023), Jamilov et al. (2023), and Jiang et al. (2024) are closely related to ours. Florackis et al. (2023) apply textual analysis tools to 10-K risk factor disclosures by firms to generate a firm-level measure of cybersecurity risk for all US-listed firms. Jiang et al. (2024) apply several machine learning techniques to a broader set of information - though including 10-K filings - to estimate the ex-ante probability that a firm will face a cyberattack. Both papers then show that their cybersecurity measure is related to stock returns. Related to this strand of research, Jamilov et al. (2023) build text-based measures of cybersecurity risk from quarterly earnings calls, finding that exposure to cybersecurity risk affects profitability, cash flow, stock returns, and tail risks in option markets both directly and via contagion effects.

As this makes clear, our evidence that cybercrime risk is priced by the stock market is not completely new to the literature. However, we believe that our simple approach has several strengths relative to alternatives while retaining an ability to explain stock returns. While we try to resist competing with these alternative approaches, we do demonstrate areas in which our cybercrime beta measures add value. In particular, our measure outperforms in a horse race with the 10-K-based cyber risk measure of Florackis et al. (2023), as discussed in section 3.2.

Perhaps most importantly, our paper extends beyond the asset pricing results. First, we examine what drives firms' exposure to cybercrime risk. Our paper adds to the corporate governance literature, highlighting that broad measures of corporate governance such as accruals relate to stock returns. More specifically, we complement recent work by Ashraf (2022) and Kamiya et al. (2021) by providing evidence that adding managerial resources to specific board level committees can enhance risk oversight and reduce a firm's exposure to cybercrime risks.

Second, our study enriches the literature by exploring risk transmission among product market peers through spillovers. Grounded in the theoretical framework of Bloom et al. (2013) and supported by empirical evidence from Tseng (2022), our analysis offers an insight into how technological advancements foster industry innovation yet concurrently unveil new systematic risks, highlighting a complex interplay between technological progress and emerging vulnerabilities.

Third, our research contributes to understanding the economic effects of digital adoption on firm growth by examining the inverse relationship between digitization and investor preferences under cybercrime concerns. Unlike studies that highlight the growth benefits of digitization and AI (Chen and Srinivasan, 2023; Babina et al., 2024), our findings suggest investors may favor less digitized firms as a risk hedge due to the strong link between digitization and cyber vulnerability. Similarly, we provide results consistent with theoretical models of the data-driven economy, including Farboodi et al. (2019), Farboodi and Veldkamp (2021) and Gomes et al. (2023). The latter, in particular, builds a model of the data economy that results in a cybercrime-driven innovation loop. Firms in the data economy protect themselves from cybercriminals by innovating more but this only serves to make their data more enticing to criminals. Our empirical results complement this work, demonstrating the nature of the relation between IT investment by firms and their exposure to cybercrime risks.

Additionally, we extend our asset pricing results into the fields of hedging and insurance. Engle et al. (2020) develop a climate change risk index using news data from *The Wall Street Journal* and construct related hedging portfolios. Similarly, we construct hedging portfolios for cybercrime risk following Alekseev et al. (2022). We use this evidence to justify upper and lower bounds on cybercrime insurance premiums chargeable in the United States, adding to the cyber insurance literature reviewed by Koijen and Yogo (2022).

Finally, our study is related to a growing literature measuring the state of the economy using business news (Baker et al., 2021; Kelly et al., 2021; Fisher et al., 2022; Bybee et al., 2023) and information extracted from the news media to predict asset returns (Tetlock, 2007; Garcia, 2013; Ke et al., 2019).[3] We add to this literature by exploring the impact of cybercrime-related narratives in public news.

The paper is organized as follows. Section 2 describes the key data used in the paper and explains how we calculate firm-level measures of exposure to cybercrime risks. Section 3 presents the cross-sectional asset pricing results that demonstrate significant risk premium. Section 4 explores factors that explain the different exposures of firms to cybercrime risks. Section 5 presents an evaluation of the hedging performance of a simple strategy around cybercrime events, and quantifies the risk premium for the cybercrime risk factor. We use these to comment on the development of cybercrime insurance markets. Section 6 summarizes our robustness checks while Section 7 concludes the paper.

[3] See also survey studies by Tetlock (2015) and Gentzkow et al. (2019).

2 Data and Initial Analysis

2.1 Refinitiv cybercrime news index

We obtain the cybercrime news index data from Refinitiv MarketPsych. Refinitiv derives news feeds of newly published content from approximately 40,000 internet news sites. More specifically, the news or social media content of information is assembled via Refinitiv crawls through hundreds of financial news sites, including, for example, *The New York Times, The Wall Street Journal, The Financial Times, Seeking Alpha* and many other sources that financial professionals widely read. In contrast to the traditional method of lexical analysis used in textual study, the technology used to create Refinitiv overcomes several shortcomings of the conventional approach broadly used in extant finance and economics studies (detailed information can be found in Peterson (2016)).

The Refinitiv cybercrime news data used in our empirical study calculates the intensity of cybercrime-related news narratives reported to the public. The index is unipolar and ranges from zero to one.[4] The higher the number, the more proportional references to cybercrime narratives in news articles. Specifically, the Refinitiv cyberCrime score is calculated by counting all cybercrime-related news references scaled by the total news references, named *Buzz* within Refinitiv. Figure 1 displays the cybercrime news index score at a daily frequency from 1998 to 2021. There are peaks on particular days for the most severe cyber incidents in the US. For example, the early notorious cyber incident happened on February 12, 2000, in which Michael Calce hacked multiple commercial websites; recent famous data breaches in September 2017 for Equifax and May 2021 for Colonial Pipeline. Additionally, the cybercrime news score varies at a daily frequency. It steadily increased from 1998 to 2021, consistent with the advancement of the internet and increasing concern about cybercrime in data implementations in the economy.

Hence, the Refinitiv cyberCrime is a fraction of total news references and scrutinizes only

[4] There are rare cases of negative values due to *Buzz* being low, and the references to those indexes are "Negated". For example, references about "anti-cybercrime measures" or "fighting cybercrime" will cause a negative value. The words "anti" and "fighting" allow companies whose business prevents or stops cybercrime not to have positive scores. However, only 30 out of 8306 days have negative values, less than 0.4% sample size. Therefore, our results are not affected by excluding days with negative values.

news stories related to cybercrime events. Based on the Refinitiv data user guide, we create the measure of cybercrime news coverage (*CCB*) by multiplying the cybercrime score and *Buzz*.

$$CCB_t = cybercrime_t \times Buzz_t \tag{1}$$

The CCB_t is calculated at a daily frequency as the measure of the intensity of cybercrime-related narratives covered by news media in the US.[5] Intuitively, the higher the value of CCB_t, the more discussion about cybercrime is reported in the news media, raising investors' awareness of cybercrime risk by reading the cybercrime news narratives.

2.2 Cybercrime news shocks

The first column in Table 1 shows that the *CCB* series is quite persistent, with an AR(1) coefficient of 0.68. Nevertheless, we reject at 1% level the null hypothesis that *CCB* has a unit root. To further investigate the potential correlation between the cybercrime news measure and other benchmark economic risk variables, the second column in Table 1 shows the results by adding ΔVIX and ΔEPU as additional controls in the AR(6) model. Indeed, our cybercrime news measure is not related to ΔVIX and ΔEPU.[6]

We apply an AR(6) model to extract cybercrime news innovations which we use as our measure of cybercrime news shock (*CCA*).[7] We first estimate

$$CCB_t = a + b_i \sum_{i=1}^{6} CCB_{t-i} + \varepsilon_t^{CCB} \tag{2}$$

using a backward-looking one-year rolling window of daily *CCB* data. We then standardize ε_t^{CCB}

[5] The daily measures from Refinitiv are calculated from newsfeeds before 3:30 PM ET each day. Please refer to detailed information about the Refinitiv news sources in the book by Peterson (2016). Additionally, this is a common feature of using news or social media data in textual analysis. Please see the survey studies about textual analysis in finance by Tetlock (2015), Loughran and McDonald (2016), and Loughran and McDonald (2020).

[6] The EPU is the economic policy uncertainty index developed by Baker et al. (2016).

[7] See related studies by Brogaard and Detzel (2015) and Engle et al. (2020). We use an AR(6) model as this reduces the autocorrelation issue, controls for potential day-of-the-week effect, and results in standardised innovations that pass both ADF and KPSS stationarity tests in each rolling window.

as follows:

$$CCA_t = \frac{\varepsilon_t^{CCB} - \bar{\varepsilon}_t^{CCB}}{\sigma_{\varepsilon_t^{CCB}}} \tag{3}$$

where $\bar{\varepsilon}_t^{CCB}$ is the mean of the cybercrime news innovation in each rolling regression sample and $\sigma_{\varepsilon_t^{CCB}}$ is its standard deviation. CCA_t is our measure of cybercrime news shocks for the one year leading up to time t. This approach ensures that we do not include any future information in the following tests.[8] The sample starts on January 1st, 1998, so our first rolling window runs from this date until December 31st, 1998.

2.3 Cybercrime exposures

Cybercrime exposures of individual stocks are obtained from regressions of daily excess stock returns on these cybercrime news shocks plus the market excess return:

$$R_{i,t} = \alpha_i + \beta_{MKT,i} R_{MKT,t} + \beta_{CCA,i} CCA_t + \varepsilon_{i,t} \tag{4}$$

where β_{CCA} is the estimated cybercrime beta. The sample matches that used to obtain the cybercrime news shock. That is, each cybercrime sensitivity is estimated using the past year of daily returns and cybercrime innovations. We only control for the market factor since Liu et al. (2021) argue that the CAPM outperforms more complicated models in testing zero alphas from a market efficiency perspective. Nevertheless, we control for many benchmark factors in subsequent portfolio sorting analyses.[9]

We examine all common stocks (share codes 10 and 11) traded on the NYSE, Amex, and Nasdaq exchanges from January 1998 through December 2021. The daily and monthly return data are from the CRSP, and we adjust stock returns for delisting effects following Shumway (1997).

[8] This standardization also benefits the following beta estimation will be more comparable since the cybercrime news coverage is different as technological progress changes dramatically in the sample period (from 1998 to 2021). For example, Figure 1 shows that samples after 2005 have relatively more cybercrime news stories.

[9] The backward-looking rolling regression with the CAPM model is also suggested by Barroso et al. (2021) to capture the conditional relationship between the state variable and the tested variables. We also estimate the $\beta_{CCA,i}$ using Fama-French three factor and Carhart models but our conclusions are unaffected.

Following Amihud (2002) and many other studies, we eliminate stocks with a price per share less than \$5. We require at least 60 trading days for a stock to be included in the analysis.

We then move the sample forward one calendar month, re-estimate both the cybercrime innovations series and the firm-level exposures to cybercrime. We continue until the sample is exhausted in December 2021. This rolling-window approach means that all estimates are based on information available to investors in real-time with no look-ahead bias. It also accounts for the increasing level and volatility of the Refinitiv cybercrime index over our sample. Standardizing the innovations using full-sample data as done by Jamilov et al. (2023) is potentially problematic given that the daily change in the Refinitiv index has a standard deviation of 0.02% in 1998 but 0.13% in 2021.

Stocks with a negative $\beta_{CCA,i}$ suffer poor returns when there are positive innovations in the cybercrime news coverage (CCB). Stocks with positive sensitivities to cybercrime news shock are hedging stocks that offer insurance against positive shocks in cybercrime news. When the public's awareness of cybercrime increases from news media reports, these stocks offer positive returns. Such hedging stocks should command a high price and hence offer a low-risk premium if investors are concerned about cybercrime negatively shifting future economic conditions or the investment opportunity set. Conversely, stocks with negative $\beta_{CCA,i}$ are more risky and exposed to cyber-related crimes, so those should command a positive risk premium.

3 Cross-Sectional Asset Pricing Results

Non-traded factors – including cybercrime news – which capture fundamental risks in the economy ought to explain the cross-section of expected returns. However, measured changes in these factors contain measurement errors. To reduce factor noise, factor-mimicking or tracking portfolios containing traded assets that represent the underlying non-traded factors are widely used (Huberman et al., 1987; Breeden et al., 1989; Ang et al., 2006; Giglio and Xiu, 2021). We follow the time-series approach of Lamont (2001) and regress the non-traded cybercrime series on contemporaneous returns of traded assets (Z_t), using the fitted values from this regression as a traded asset-based proxy for cybercrime for each one-year long rolling regression window:

$$CCA_t = c + b'Z_t + u_t \tag{5}$$

The traded assets we use are five portfolios sorted according to sensitivities to the cybercrime news shock estimated as described in the previous section. All portfolios are value-weighted and we use NYSE stock break-points throughout. Because the traded assets are excess returns, the coefficients in the vector b can be interpreted as weights in the zero-cost portfolio. For each regression window, we construct the daily tracking factor return factor, $b'Z_t$, which we denote $TCCA_t$.

$$TCCA_t = b'Z_t \tag{6}$$

The tracking portfolio $TCCA$ contains the portfolio of asset returns maximally correlated with realized innovations in cybercrime news coverage using a set of basis assets with different exposures to cybercrime news shock (β_{CCA}). By virtue of this mimicking factor, the primary advantage of using $TCCA$ in the following analysis to measure the aggregate cybercrime risk is that we have a good approximation of innovations in cybercrime news, and allows us to alleviate the issues caused by noise in the news data.

Figure 2 presents the average daily Pearson correlation between CCA_t and the cybercrime news shock tracking portfolio returns is around 0.54 from the 276 regression windows. The correlation ranges from 0.26 to 0.72. Figure 3 displays time-varying weights (b) for the five portfolios. On average, the weights of portfolio 5 are always positive and the average weight on portfolio 5 is close to +0.95. In the meantime, the weights of portfolio 1 are always negative and the average weight on portfolio 1 is close to -0.86. Additionally, the average weights on each portfolio are also monotonically increasing. Together, these results suggest that the tracking portfolio indeed efficiently tracks innovations in cybercrime news (CCA) in a manner consistent with expectations.

3.1 Tracking factor performance

We next estimate time-varying stock-level sensitivities to the cybercrime news shock tracking factor ($TCCA_t$), rather than to the non-traded cybercrime news shock proxy itself.

$$R_{i,t} = \alpha_i + \beta_{MKT,i} R_{MKT,t} + \beta_{TCCA,i} TCCA_t + \varepsilon_{i,t} \tag{7}$$

Rolling one-year regressions of returns on the market excess return and the $TCCA$ generate cybercrime tracking betas (denoted $\beta_{TCCA,i}$) that are used to allocate stocks to one of five portfolios. We then examine the returns on these portfolios in the following month. The results are reported in panel A of Table 2. As we move from Portfolio 1 to Portfolio 5, value-weighted average portfolio betas rise from -0.66 to +0.81 in a relatively symmetric pattern. Next-month average excess returns decrease monotonically from 1.08% to 0.14% per month. The returns of individual stocks in Portfolio 1 correlate negatively with shocks to cybercrime news mimicked by $TCCA$, and so risk-averse investors require higher expected returns to hold these stocks. Conversely, as the stocks in Portfolio 5 correlate positively with increased shocks in cybercrime, they are viewed as hedge stocks that perform well in times of increased risk related to cybercrime. Hence, investors pay higher prices for these stocks and willingly accept lower returns.

The average return difference between the highest and lowest beta portfolios is -0.95% per month with a Newey and West (1987) t-statistic of -2.93. The alpha analysis reported in columns 3-6 show that irrespective of the factor model used, monthly alphas from Portfolio 1 are around 0.4% and statistically significant, falling to around -0.60% for Portfolio 5 (again with large t-statistics). The high-minus-low portfolio return alphas are similar to the raw return and are again statistically significant.

This significantly negative cybercrime premium is consistent with the intertemporal capital asset pricing model of Merton (1973). An unexpected increase in cybercrime (and cybercrime news) adversely affects future investment and consumption opportunities. Investors prefer to hold stocks whose returns increase upon such unfavorable events and thus hedge their exposures to cybercrime.

That is, they compensate for reduced consumption and weakened future investment opportunities by holding stocks that positively correlate with cybercrime. This intertemporal hedging demand implies that investors are willing to pay higher prices and accept lower returns for stocks with higher cybercrime betas.

It is noticeable from Table 2 that irrespective of the pricing factor model used, the majority of the negative alpha in the high-minus-low portfolio comes from the high cybercrime beta leg (Portfolio 5). This proportion is never below 60% and in the case of the Fama-French five-factor model, is as high as 64%. Stocks in portfolio 5 are the hedges that tend to offer high payoffs when cybercrime news increases and these stocks offer typically low expected returns as a result of this hedge characteristic.

We next examine the relation between cybercrime sensitivities and next-month stock returns controlling for well-known cross-sectional return predictors. We perform bivariate portfolio sorts on the cybercrime tracking beta (β_{TCCA}) in combination with the market capitalization (SIZE), book-to-market ratio (BM), operating profitability (OP), investment (I/A), market beta (β_{MKT}), market volatility beta (β_{VIX}), economic policy uncertainty beta (β_{EPU}), momentum (MOM), short-term reversal (ST), illiquidity ($ILLIQ$), idiosyncratic volatility ($IVOL$), and analyst dispersion ($DISP$).[10] We first form five portfolios based on the predictor variables. Then, within each predictor portfolio, we sort stocks into five portfolios based on the cybercrime beta (β_{TCCA}) so that portfolio 1 (portfolio 5) contains stocks with the lowest (highest) cybercrime beta values. We then average the next month's value-weighted portfolio returns across the five predictor portfolios for each of the five cybercrime beta portfolios. This creates a set of five portfolios with very similar levels of the predictor variable but which differ by cybercrime beta.

We report value-weighted portfolio results from these conditional bivariate sorts in Panel B of Table 2. The first column shows that after controlling for size, the α_8 controlling FF five-factors, momentum, short-term and long-term reversal factors tends to fall as the cybercrime tracking port-

[10] Financial variables are obtained from the merged CRSP-Compustat database. Analysts' earnings forecasts come from the Institutional Brokers' Estimate System (I/B/E/S) data set. Benchmark pricing factors and testing portfolios are downloaded from related data libraries.

folio beta increases from portfolio 1 to 5. The high-minus-low portfolio alpha is about -0.7% per month with a Newey-West t-statistic in excess of 2.3. Subsequent columns of Panel B, Table 2 show a very similar pattern and in most cases, the high-minus-low alpha is even greater than that seen when controlling for size. Statistical significance is strong for all predictors.

Our key findings are confirmed when we apply the alternative technology of Fama and MacBeth regressions (1973) of the realized excess return of stock i in month $t+1$ on the cybercrime tracking portfolio beta of stock i in month t and the collection of stock-specific control variables observable at time t considered in Panel B of Table 2. These cross-sectional regressions are estimated monthly from January 1999 to December 2021.

The univariate regression results reported in the first column of the left panel in Table 3 indicate a negative and statistically significant relation between the cybercrime beta and the cross-section of future stock returns. The average slope is -0.46 and highly significant. Were a stock to move from Portfolio 1 to Portfolio 5, all other things equal the expected return of that stock would decrease by a substantial 0.68% per month [-0.46×(0.66-(-0.81))]. The remaining columns,(2)-(4), show that while adding several fundamental control factors reduces the magnitude of this coefficient, it remains sizeable and statistically significant.

Moreover, we further explore the role of non-tech firms in driving the observed negative return predictability. Drawing from the study by Chen and Srinivasan (2023), we differentiate firms into tech or non-tech industries based on the SIC, NAICS, and GICS codes. Specifically, a dummy variable is assigned the value one when firms are in the defined non-tech industry and zero otherwise. We expect that non-tech firms, traditionally less dependent on digitalization, might exhibit a stronger negative relationship between cybercrime beta and future stock returns. This is confirmed by the results reported in column (5), where the interaction term ($D_{nontech} \times \beta_{TCCA}$) reflecting non-tech firms' cybercrime beta is significantly negative. Column (6) reaffirms these results, even when accounting for potential industry effects, suggesting that non-tech firms' inherent characteristics, notably their lower reliance on digitization, play a pivotal role in shaping the impact of cybercrime betas on stock returns. These insights lay the groundwork for an in-depth exploration of the relationship between firm digitization and cybercrime beta in section 4.4.

In our final set of asset pricing tests, we investigate whether cybercrime tracking betas have the same predictive power for the cross-section of equity portfolios. We obtain portfolio daily return data on 49 industry portfolios and three sets of portfolios from sorts based on size and book-to-market, size and investment, and size and profitability from Kenneth French's data library. These 349 portfolios are widely used in the literature since they generate significant cross-sectional differences in portfolio expected returns (Bali et al., 2017).

We estimate rolling cybercrime betas for each portfolio controlling for Fama-French five factors.[11] Univariate portfolio sorting results are presented in Table 4. Portfolios sorted by β_{TCCA} provide results consistent with those from individual stocks. As the average cybercrime tracking beta increases from portfolio 1 to 5 one-month ahead expected returns decrease monotonically. The H-L portfolio generates expected returns of -0.3%. The difference in risk-adjusted returns (α) between high and low β_{TCCA} portfolios is significantly negative, and the magnitude is about -0.25% and consistent across different pricing models. Again, we note that the alpha is concentrated in the high beta portfolio.

We conclude that the cybercrime tracking beta is priced not only in the cross-section of individual stocks but also in the cross-section of equity portfolios. One can also infer that hedging against cybercrime can be implemented via portfolios rather than diving into the entire stock universe, which is relatively costly.

3.2 Discussion

In summary, we have presented results demonstrating that firm-level sensitivity to innovations in cybercrime news are robustly priced in the cross-section of US equity returns. That cybercrime risk is priced is not new to the literature. For example, Florackis et al. (2023) and Jiang et al. (2024) both report similar findings. However, we believe that our approach to measuring firm-level exposures has several benefits.

[11] The results are not sensitive to use the other models for our beta estimation.

First, both papers apply sophisticated text analysis tools to extract firm-level measures of cybersecurity exposures. Florackis et al. (2023) consider 10-K risk factor disclosures while Jiang et al. (2024) consider a broader set of information - including 10-K filings - to estimate the ex-ante probability that a firm will face a cyberattack. Relatedly, Jamilov et al. (2023) build text-based measures of cybersecurity risk from quarterly earnings calls. In contrast, we estimate firm-level cybercrime exposures from simple regressions of returns on news innovations. The simplicity of our approach has several advantages, not least the ability to be applied in jurisdictions with less rigorous regulatory filing requirements and/or less informative disclosures through analyst calls than in the United States. We provide reassurance that the choice of cybercrime measure is not critical by generating very similar findings using publicly-available Google search data in the robustness analysis below. The simplicity of our approach does not mean inferiority. Our cybercrime tracking beta outperforms a horse race with the yearly firm-level 10-K cyber risk exposure measure of Florackis et al. (2023) in hedging significant cyber incidents. The results provided in Appendix B, demonstrate that our measure has a clear edge in pricing returns in cross-section based on investors' demand for hedging cybercrime risk.

Second, these three papers each build firm-specific measures of exposure to cybersecurity risk. As such, they naturally conflate idiosyncratic and systematic cybersecurity risks. Our analysis differs since we estimate firms' sensitivities to a common measure of cybercrime reported in news articles. While we acknowledge that there are a variety of measures of cybercrime risk from which to choose, having made this selection we follow standard and transparent techniques to derive firm-specific sensitivities to cybercrime risk.

Our approach has some other advantages. Florackis et al. (2023) use data beginning in 2007, at which time fewer than 30% of U.S. firms make cybersecurity-risk disclosures in their 10-K filings. This proportion jumps from 39% in 2010 to over 60% in 2012 following specific guidance from the SEC in 2011. Whether firms' managers chose to disclose the true cyber-risks they faced appears to have been at least partially driven by regulatory requirements for a large part of their sample. Of course, there is also the question of whether firms' managers can accurately assess the cyber-risks that they face given the novelty of this particular risk and the fast rate of change of both vulnerabilities to cybercrime and the scale of the activities of cyber-criminals. In particular, vulnerabilities due to supply chain linkages may be important. Managers of a particular firm may not feel it to be much at risk from cybercrime, but performance may well be impacted by cybercrime attacks either up- or down-steam in its supply chain. Rather than using managers' disclosed assessments of own firm and spillover risks, we rely on the market's assessments of cybercrime risks as evidenced by stock returns.

Perhaps most importantly, our paper differs in terms of the emphasis we place on firms that offer a hedge for cybercrime, rather than focusing on the positive risk premium demanded by investors to hold positions in stocks most vulnerable to cyber attack. The key measure in Jiang et al. (2024) is an ex ante estimated cyber attack probability for the following year, naturally bounded at zero. Florackis et al. (2023) compute a cybersecurity risk index for each firm which takes the value zero up to at least the 25th percentile of their sample. In these two applications, firms cannot act as hedges for cybercrime risks, they can only be said to be at less risk than other firms. In our paper, the distribution of estimated exposures to cybercrime risk is reasonably symmetrically distributed around zero. While we find a significant positive Fama-French five-factor alpha for the portfolio of firms with the most negative sensitivities to innovations in cybercrime news, we find large and very statistically significant negative alphas for the portfolios of firms with hedging properties. We note that this is also true – though less emphasised – in the existing literature. Jiang et al. (2024), for example, note that most of their alpha "comes from the bottom decile portfolio, where stocks with lowest cyber risk reside."[12]

3.3 Next steps

Having demonstrated the power of our simple measure to explain the cross-section of US stock returns, and placed these in the context of related work also addressing asset pricing effects of

[12] Florackis et al. (2023) consistently find significant underperformance of their low cyber-risk portfolio with a cybersecurity risk index of zero. Their high cyber-risk portfolio (index = 0.46) only commands a positive alpha in a value-weighted setting.

cyber risks, our paper now reaches a fork.

In the following section we take the asset pricing results as given and move on to ask what factors drive firms' differential exposure to news innovations about cybercrime. In doing so, we explore how strong corporate governance, product similarity, and financial decisions related to digital adoption and IT investments impact a firm's cybercrime risk exposure and affect asset pricing. Our aim is to gain a clear understanding of these factors, examining their contributions to the context of investor valuation regarding firms' cyber risk exposure in financial markets.

In Section 5, we return to the asset pricing results and travel in a different direction, using them to construct and evaluate the performance of an insurance-like hedging strategy across a large set of cyber events affecting the US economy. Having demonstrated the encouraging performance of the hedging portfolio, we extend the asset pricing results further to estimate an ex-post cybercrime risk premium and use this to place indicative upper and lower bounds on the size of the market-wide premium insurers could charge.

4 Attributes of Cybercrime Hedging Stocks

A fundamental question arises: What drives investor evaluations of firms' exposure to cybercrime risk. Specifically, what are the determinants of cybercrime betas? Focusing on the nature of cybercrimes and the strategies for insuring against them, this section emphasizes the efficacy of corporate governance and the nuances of organizational strategies, which include product development, digitalization, and IT infrastructure investment, especially during periods of heightened cybercrime concern in the market. We focus on four dimensions of firm decisions that potentially contribute to the variations in cybercrime beta.

First, building on papers including Johnson et al. (2000) and Mitton (2002) which note the outperformance of stocks with better corporate governance in the face of negative economic shocks, we examine the link between corporate governance quality and cybercrime betas. We find that a broad brush proxy for corporate governance quality (accruals), a more specific human capital measure of board level risk management resources, and higher ESG-based governance scores each relate as expected to cybercrime betas.

Second, we combine the methodological framework of Hoberg and Phillips (2016) regarding product similarity with firm-level cybercrime news data to assess the implications of cybercrime spillovers among peer groups of firms identified by product similarities. Our findings reveal that investors tend to ascribe higher valuations to firms with less product market overlap with cybercrime news-reported peers over a one-year rolling window.

Third, constructing a novel measure of a firm's digitization, we explore its dual impact on a firm's digital activity and cyber vulnerability. While digitization fosters growth for firms, it simultaneously heightens their exposure to cyber threats. Our analysis contributes to understanding the balance firms must strike between leveraging digital innovations for economic gains and managing the associated cyber risks, offering insights into the economics of cybersecurity in the digital age.

Finally, we build upon the theoretical framework of Gomes et al. (2023) on the data-driven economy, focusing on the 'innovation loop' within data-centric firms. Firms focused on digital innovation, report elevated digitization-related expenditures and high IT investment, amplifying their exposure to cyber risks. Conversely, firms with a less pronounced focus on data, demonstrated by lower relative IT spending, tend to exhibit diminished cyber risk. Our empirical analysis of firms' IT investment data substantiates these dynamics, providing evidence that these factors are important in shaping investors' assessments of cybercrime risk exposures.

4.1 Periods of heightened cybercrime concern

We utilize the Refinitiv MarketPsych cybercrime news index to define periods of significant market concern regarding cybercrime (*HCCR*) through a moving average crossover approach.[13] This method allows for a nuanced identification of times when cybercrime news intensity surpasses

[13] This moving average crossover technique parallels the study by Bybee et al. (2023), which constructs narrative shocks by selecting specific windows that capture heightened attention to narratives. Additionally, Huynh and Xia (2021) employ a similar empirical approach to explore the factors influencing investor valuation of bonds during periods of heightened climate change news risk.

historical norms, signaling increased market attentiveness to cybercrime issues. To do this, we calculate the average value of cybercrime news coverage for each month and compare it to the trailing 90-day moving average. A dummy variable is assigned a value of one to denote months where the average cybercrime news coverage exceeds this 90-day benchmark. This method allows us to differentiate between periods of intense cybercrime news coverage and comparatively quieter times. Such a distinction is crucial in our investigation into the key determinants that influence investor valuation of firms, particularly during periods when intensified reporting on cybercrime significantly raises investor awareness and impacts their response to the associated risks.

Figure 4 presents a heatmap illustrating the disparity between the monthly average of cybercrime news coverage and the preceding 90-day moving average. The intensity of the color corresponds to the magnitude of this difference; a warmer color indicates a greater disparity in cybercrime news coverage between the current month and the past three months. Notably, certain months correlate with significant cyber incidents.[14] Consequently, given the escalating concerns about cybercrime as reflected in news media, the following sections delve into the impact of intensified cybercrime news coverage on investor valuation, particularly in terms of hedging against prospective cybercrime risks.

4.2 Corporate governance and cybercrime

In a speech on “Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus” given on June 10, 2014, Commissioner Luis Aguilar of the Securities and Exchange Commission (SEC) emphasized the role of effective boards of directors with oversight for the rising risk of cyberattacks, and that strengthened corporate governance can offer benefits to stakeholders and the integrity of the capital market.[15] This speech motivates us to explore whether good corporate governance explains why hedging stocks outperform following cyberattacks.

[14] For instance, February 2000 was marked by multiple online hacking cases orchestrated by Michael Calce; June 2011 witnessed a cyberattack on CITI Bank; September 2017 was notable for the major data breach at Equifax; December 2020 saw a data breach within the US federal government; and the most recent incident in our dataset, the Colonial Pipeline ransomware attack, occurred in May 2021.

[15] The article is available at https://www.sec.gov/news/speech/2014-spch061014laa

We use three measures of the quality of corporate governance. Our first measure, accruals, is commonly used as a proxy for general governance quality in the corporate finance literature (Sloan, 1996; Larcker and Richardson, 2004; Pedersen et al., 2021). The lower the accruals are, the better corporate governance is deemed to be. In our statistical analysis, we therefore take the negative of accruals such that a higher value suggests better governance.

Columns (1) and (2) in Table 5 demonstrate a highly statistically significant positive relation between the interaction term $HCCR \times$ Accruals and β_{TCCA}. This indicates that strong corporate governance, marked by lower accruals, effectively reduces a firm's cybercrime risk, thereby enhancing its stock value in times of elevated cybercrime news.[16]

Our second measure is the Governance component of companies' ESG scores, sourced from Refinitiv Workspace and spanning the years 2002 to 2021. We categorize firms into low, medium, and high Governance groups based on the tercile distribution of annual data.[17]

The findings, as shown in Columns (3) and (4) of Table 5, align with the patterns observed in columns (1) and (2), demonstrating a positive link between governance strength and cybercrime beta. Specifically, an elevation in governance to a higher category correlates with an approximate 2.5% increase in cybercrime beta, relative to the within-firm standard deviation.

Concerned that missing Governance scores in the early part of the sample affect our results, we draw on the work of Lee et al. (2015) which underscores the significant correlation between a firm's financial fundamentals and those of its industry peers. Specifically, we replace missing Governance scores with the median score within each firm's Standard Industrial Classification (SIC) industry for each year. The results, detailed in Column (5) are consistent with those obtained from the smaller sample. Enhanced governance mitigates cybercrime risk across firms.

Accruals and the general Governance score are both relatively coarse measures of corporate governance quality that do not have a specific cybercrime or risk focus. Therefore, our third mea-

[16] This general result parallels the finding that socially responsible firms face less credit risk and recover faster (Lins et al., 2017; Albuquerque et al., 2019).

[17] The data coverage is uneven, particularly before 2015, with fewer firms included in earlier years. Using categorized variables helps address this imbalance, ensuring that the regression model remains robust across years with varying amounts of data.

sure of corporate governance is the number of experts on firms' boards who are experienced in risk management or knowledgeable on information, technology, and/or cyber-related issues. This human capital-focused measure echoes Aguilar (2014). It is also in line with Kamiya et al. (2021) and Ashraf (2022) who stress that improving corporate governance by having more risk management committee members or information security experts on the board can significantly enhance cyber risk oversight of the firm and reduce its risk exposure to cybercrime.

For the human capital measure, we obtain board committee members' data from BoardEx, and identify members with roles related to cybercrime risk management by manually scrutinizing each member's committee roles for keywords related to risk management, corporate governance, or informatics. Specifically, we select committee names including words with "risk"(R), "security"(S), "governance"(G), "operation"(O), "information"(I),"technology"(T), "data"(D) and "cyber"(C). To focus on more operational risk management and information-related expertise, we exclude committees that mention financial risks, such as credit risk, audit risk, and names that are environment-related. With the relevant RSGOITDC committees identified, we count the number of distinct members.[18]

We examine the relationship between cybercrime beta and corporate governance measures, focusing on periods with high cybercrime news coverage. Essentially, we regress β_{TCCA} on the interaction term between $HCCR$ defined above and lagged measures of corporate governance, including accruals or the intensity of human capital investment indicated by the number of RSGOITDC experts. Regressions also include a set of stock-level control variables and key firm financial metrics such as leverage ratio and return on assets (ROA).[19] All regressors are standardized to have zero mean and unit standard deviation for consistency.

The results for RSGOITDC are presented in columns (6) and (7) of Table 5. We consider a simple count of RSGOITDC committee members, denoted by 'Expert'. The interaction term

[18] We take the logarithm for the number of experts plus one to reduce skewness. However, the results remain unchanged without taking logarithm.

[19] All corporate governance measures and control variables are lagged for one fiscal year or one period to avoid any look-ahead bias.

HCCR × Expert is positive and significant at the 1% level.[20]

The economic magnitudes of these effects are also meaningful. In our quantification of economic impacts, we consider the fixed effects of 'cybercrime beta,' which, though present, are relatively modest, alongside the more significant effects associated with 'Expert'. The fixed effects are stronger for the experts headcount, meaning that according to Liu and Winegar (2023) and Mitton (2024) would ought not overstate the magnitude of a "reasonable" shock to the key variable and instead consider an increase of just two experts, equivalent to one within-firm standard deviation. This results in an increase in the cybercrime beta of 0.02, or 4.3% of its within-firm standard deviation. However, as a policy recommendation for firms looking to improve their stock's sensitivity to cybercrime shocks, we consider the addition of a handful of experts to the important management committees of firms to be feasible and so view both of these estimates of the economic magnitudes to be conservative.

These findings highlight the crucial role of strategic human capital investment in fortifying corporate governance, risk, and informatics management, thereby effectively reducing a firm's vulnerability to cybercrime risks in periods of intensified cybercrime news reporting.

In sum, a positive relationship exists between cybercrime beta and corporate governance, especially when corporate governance is proxied by the number of experts knowledgeable in risk oversight and informatics in top management. Fostering better corporate governance by placing experts in top management roles helps firms shield themselves from cybercrime risks. The results of our study shed light on related work by Kamiya et al. (2021) and Ashraf (2022), contributing a new insight into the impact of corporate governance on cyber-related incidents. Put simply, effective investment in human capital expertise can help mitigate the effects of cyber attacks.

[20] We also consider the ratio of RSGOITDC experts to total committee members, 'Expert%', and its interaction with *HCCR*. The results are essentially unchanged from those reported for the simple count of experts.

4.3 Peer firms, product market, and cybercrime

Investors actively seek information from firms within the same industry, particularly those with fundamental similarities across various dimensions. This behavior, underscored by the significant cross-sectional return predictability, suggests a firm's responses to common market shocks are closely aligned with its peer firms (Lee et al., 2015). In a related vein, our investigation considers the concept of economic affinity and its impact on asset pricing, focusing specifically on how product market connections influence firms' cybercrime risk exposure.[21]

Leveraging a unique firm-level cybercrime news index, we investigate the impact of peer firms' cybercrime news on investor valuation concerning systematic cybercrime risk. For each firm, we pinpoint peer firms based on product similarity. We then identify the intensity of cybercrime news relating to that peer group. We posit that firms with fewer peers mentioned in current cybercrime news articles are perceived by investors to have lower risk. During times of heightened concern over cybercrime, such firms are considered to be safer havens by investors which, in turn, could bolster their market valuation.

We use Hoberg and Phillips (2016)'s dynamic text-based measure to identify industry peers.[22] Each year, they extract the product descriptions from the 10-K filings of all firms in the sample, and identify the M unique words in the union of all descriptions.[23] Focal firm i's vocabulary is represented by the vector P_i of length M, where each element takes the value one if the firm uses the given word, and zero otherwise. The product similarity score, $PS_{i,j}$ for focal firm i and firm j is the dot product of normalized vectors for firms i and j and is bounded [0,1]. The product similarity score is higher when firms i and j use more of the same words. Firm pairs with product similarity scores above a threshold level are defined to be peers. Based on this, the N peer group firms of focal firm i are defined, and the product similarity values, $PS_{i,j,t-1}$, are collected for all N

[21] See related studies by Hou (2007), Cohen and Frazzini (2008) and Cohen and Lou (2012) on return predictability based on close economic affinities.

[22] See related studies by Foucault and Fresard (2014), Cao et al. (2019), and Cao et al. (2021) using text-based measure of Hoberg and Phillips (2016) to identify firm industry peers.

[23] They keep only nouns and proper nouns, and exclude common words and geographic terms as explained in Hoberg and Phillips (2016).

peer firms.[24]

The firm-level cybercrime news index, sourced from Refinitiv MarketPsych, provides individual firm reports that allow us to identify firms mentioned in cybercrime news articles.[25] For focal firm i, we check whether each of its N peer firms are mentioned in cybercrime news articles in the previous year. For peer firm j, an indicator variable I takes the value one if it is mentioned in at least one article, zero otherwise.

Combining product similarity scores and firm-level cybercrime news indicators, we calculate a novel metric, the Product Similarity Peer firm Cybercrime News (PSPC) as:

$$PSPC_{i,t} = \frac{\sum_j^N PS_{i,j,t-1} \times I_{j,t}}{\sum_j^N PS_{i,j,t-1}} \quad , \tag{8}$$

where, $PS_{i,j}$ represents the product similarity of firm i to peer group firm j, and I_j is an indicator variable that takes the value 1 when firm j is mentioned in cybercrime news. $PSPC$ lies between 0 and 1, and is increasing in the number of peer group firms that are mentioned in cybercrime reports, and increases if closer competitors, rather than more distant ones, are mentioned in cybercrime news reports.

The $PSPC$ metric thus reflects the focal firm's product market overlap with firms implicated in cybercrime news, ranging from 0 (no overlap) to 1 (complete overlap).[26] Moreover, accounting for a firm's overall product similarity allows for a comprehensive analysis, enabling investors to evaluate the entire product market spectrum in which the focal firm operates. As highlighted by Cohen and Lou (2012), the complexity arising from a firm's engagement across diverse markets can complicate investor understanding, making it more challenging to process information for conglomerate firms compared to their monoline or niche counterparts. This aspect underscores the interplay between product market diversity and investor perception of cybercrime risk.

Our proposition is that firms with less cybercrime news relating to firms present in their prod-

[24] To mitigate look-ahead bias, we employ the Hoberg and Phillips measure lagged by one fiscal year.

[25] The yearly distribution of firm-level cybercrime news is in Figure 5.

[26] If the focal firm's business only spans the product markets where the cybercrime news reported peers to operate, as $\sum_j^N PS_{i,j,t-1} \times I_{j,t} = \sum_j^N PS_{i,j,t-1}$, the $PSPC_{i,t}$ equals 1. On the contrary, if the focal firm's product is totally distinct to cybercrime news reported firms, the $\sum_j^N PS_{i,j,t-1} \times I_{j,t} = 0$ and the $PSPC_{i,t} = 0$.

uct markets are considered to have lower cybercrime risk exposures. During periods of heightened cybercrime concerns, firms with lower PSPC values should be perceived by investors to be less vulnerable to cybercrime risk, positively influencing their market valuation. This is examined through regression analyses similar to those in section 4.1, incorporating financial controls like R&D and intangible assets to account for innovation influences.

The regression results are presented in Table 6.[27] Columns (1) and (3) demonstrate a statistically significant negative relation at the 1% level between the interaction term $HCCR \times PSPC$ and β_{TCCA}. Continuing to follow the recommended approaches of Liu and Winegar (2023) and Mitton (2024), a reduction in product similarity to peers involved in cybercrime news by one within standard deviation, approximately 10% in terms of PSPC, results in a 4.29% increase in the firm's cybercrime beta relative to its own within standard deviation.[28] This confirms that firms with fewer product market peers involved in cybercrime news are more highly valued by investors during times of heightened cybercrime concerns. This relation also holds when we take the logarithm of *PSPC* to mitigate potential data skewness, as shown in columns (2) and (4). To further demonstrate the reliability of our results, we adjust our approach by simplifying the product similarity measure, focusing solely on the count of peers within cybercrime news narratives versus the total peer count. The consistent findings across columns (5) to (8) reinforce the notion that firms with less product market overlap with cybercrime news-reported peers are perceived as shielded from industry-wide common shocks induced by cyber threats.

Our findings suggest that the pervasive nature of cybercrime, as evidenced through peer firms' news narratives, acts as a conduit for negative spillovers, overshadowing the potential competitive advantages from product market rivalry as highlighted by Bloom et al. (2013). The amplified effects of cyber threats, modeled by Eisenbach et al. (2022), resonate with our findings, underscoring the heightened vulnerability within interconnected financial sectors. Similarly, Jiang et al. (2024)'s exploration of negative responses among peer firms to cyber incidents, mediated by data similarity,

[27] All regressors are standardized to have zero mean and unit standard deviation for consistency.

[28] The net effect of PSPC is calculated as the sum of $HCCR \times PSPC$ and $PSPC$, then divided by the within standard deviation of β_{TCCA} which is 0.7. The within standard deviation of PSPC is approximately 10%.

aligns with our analysis, revealing how shared service and product offerings can serve as conduits for risk dissemination. Our investigation extends these discussions by specifically addressing how investors recalibrate their valuation of firms in light of their susceptibility to cybercrime, as influenced by their competitive positioning within product markets. The interconnectedness, suggests a collective exposure to cyber risks, necessitating a nuanced investor assessment of firm resilience.

4.4 Digitization and cybercrime

In an era of digital transformation, the adoption of artificial intelligence and digital technologies by firms has garnered significant scholarly interest for its economic impact. Babina et al. (2024) reveals that AI investments are linked to significant growth in sales, employment, and market valuation due to increased product innovation. Similarly, Chen and Srinivasan (2023) investigate the positive valuation effects of digital technology adoption in non-tech firms. However, these digital advancements also introduce vulnerabilities, a concern echoed by The Global Risks Report WEF (2022), which highlights the balance between digital innovation and cybersecurity risks.[29] Therefore, we posit that while digital technologies boost firm performance, they also heighten exposure to cyber threats, influencing investor valuations amidst varying degrees of firm digitization.

Addressing the challenge of quantifying digital technology adoptions, we apply Chen and Srinivasan (2023)'s approach, constructing a firm-level digital activity metric from conference call scripts using a defined set of digital terms spanning 2002 to 2021. Figure 6 displays the word cloud, highlighting the prominence of "IoT" (Internet of Things) and other AI-related terminology, which collectively illustrate the evolving digital landscape within corporate strategies. To accurately capture digital engagement while minimizing overlap with cyber risk indicators, we exclude big data-related terms in our analysis.[30]

[29] Chapter 3 of the WEF 2022 Global Risk Report, titled "Digital Dependencies and Cyber Vulnerabilities," highlights the increasing reliance on digital technologies and the corresponding rise in cyber vulnerabilities. It discusses how this growing digital interconnectedness exposes economies and societies to new risks, emphasizing the need for robust cybersecurity measures to protect against potential cyber threats. The chapter is instrumental in understanding the complex relationship between digitalization and cybercrime, providing a foundation for exploring how digital advancements can both drive progress and introduce new risks.

[30] Specifically, the digital terms contain five major topics, including analytics, artificial intelligence (AI), cloud (-

Beginning in January 2003, we aggregate quarterly digitization metrics from the previous year for each firm's digitization level (Digital), employing a yearly rolling window to ensure timeliness and avoid look-ahead bias.[31] To address initial data skewness caused by lots of zeros, we also apply quantization to Digital, following Chen and Srinivasan (2023). Our hypothesis is that as firms intensify their digital activities, their vulnerability to cyber threats may increase, leading investors to prefer less digitized firms as a hedge against cybercrime risk during periods of increased reporting in news media. This suggests an inverse relation between firm digitization and cybercrime beta (β_{TCCA}).

Table 7 presents the regression results.[32] The interaction terms $HCCR\times$ Digital and $HCCR\times$ QDigital in columns (1) and (4) show a significantly negative relationship between a firm's cybercrime beta and digitization. During high cybercrime news coverage periods, a one-within standard deviation decrease in the firm's digitization (Digital) raises the cybercrime beta by 4.1% of its within standard deviation, suggesting reduced exposure to cybercrime risk. Moreover, a shift from higher to lower digitization levels (QDigital) increases cybercrime beta by 8.22% of its within standard deviation, reinforcing the protective hedging effect of low digitization during periods of intensified cybercrime news.[33]

We control for the effects of intangible assets and productivity, as measured by sales per employee, to isolate the impact of firms' digitization investments.[34] Results in columns (2) and (5) confirm consistent outcomes even after controlling for these factors. As digitization can be viewed as an intangible asset, we add $HCCR \times$ Intangibility in columns (3) and (6). The results

computing), digitization, and machine learning (ML) proposed by Chen and Srinivasan (2023). As stated by Jamilov et al. (2023) and Florackis et al. (2023), data-related keywords are ranked as the most frequent keywords to measure cyber risk. Therefore, we exclude such terms to make our measure less confounding with cyber risk measures. The firm-level measure is constructed by counting the topics-related words mentioned in conference calls.

[31] Using past four-quarter digitization data from conference calls assures that investors make decisions at quarter t only have information up to $t-1$, thus without look-ahead bias and conservative for information availability. We take the logarithm for Digital to reduce positive skewness in the data.

[32] All regressors are standardized to have zero mean and unit standard deviation for consistency.

[33] The net effect of digitization is calauted as the sum of $HCCR\times$ Digital (QDigital) and Digital(QDigital), then divided by the within standard deviation of β_{TCCA} which is 0.73 in this sample.

[34] This consideration is crucial as digitization expenditures often contribute to a firm's intangible assets and can significantly enhance productivity. By adjusting for these factors in our regression models, we ensure the robustness of our findings regarding the adoption of digitization, demonstrating its distinct influence beyond the contributions of intangible assets and productivity enhancements.

for digitization are unchanged, maintaining a significant inverse relationship with cybercrime beta despite any potential positive correlation of intangible assets with cybercrime risk.

Overall, the empirical evidence highlights the crucial role of digitization in shaping firms' cyber risk profiles. Notably, the inverse relation between digitization and cybercrime beta echoes the results in columns (5) and (6) of Table 3, highlighting the implications of non-tech firms' hedging potential against cyber risks.

4.5 IT investment and cybercrime beta

Following our exploration of digitization's broader implications for firm vulnerability to cybercrime in Section 4.4, we narrow our focus to the realm of IT investments. While digitization encompasses a broad range of digital activities and transformations within firms, IT investments represent a targeted allocation of resources towards information and communication technology infrastructure, including cybersecurity measures. This distinction is crucial as we delve into the relationship between IT expenditures and firms' susceptibility to cyber risks.

Brynjolfsson and McElheran (2016) highlight that firms' IT investments are a foundational element for firms that adopting data-driven decision-making. A recent theoretical study by Gomes et al. (2023) extends the models by Farboodi et al. (2019) and Farboodi and Veldkamp (2021) and builds a model of the data economy in which data helps firms optimize their business processes whilst being subject to risk of damage by cyber criminals. The authors propose a cybercrime-driven innovation loop in which firms can hedge against cybercrimes by innovating more, but which only serves to make data even more valuable for cybercriminals. This model suggests a complicated relation between a firm's investment in data technology and its sensitivity to cybercrime.[35]

To examine the impact of IT investments on firms' cyber vulnerability, we use IT spending data from the Harte Hanks Market Intelligence Computer Intelligence Technology database. This granular data covers firm IT spending at the site level, with over 30 million yearly observations

[35] Kamiya et al. (2021) study the connection between firm characteristics and the likelihood of cyber attacks, finding that firms most likely to be attacked firms are large, are more profitable, are less risky, have higher growth opportunity, have higher leverage and asset intangibility, and make less investment in capital expenditures and R&D.

from 2012 to 2021.[36] We use the firms' estimated total spending on hardware, software, services, and communications. We would like to aggregate each site's IT spending to the firm level using the Enterprise ID code in the data set. Unfortunately, for some firms, this ID is not unique because the company names are recorded with minor differences.[37] To overcome this issue, we use the company name (GVKEY) used in the Compustat link table to match all companies in the Harte Hanks database. To assign the GVKEY to firms in Harte Hanks, we merge the two datasets by matching company names with a cosine similarity algorithm. We restrict the similarity score to at least 0.67 to ensure matching accuracy.[38] Once matched, we aggregate each firm site's IT investment using GVKEY to obtain its yearly IT spending. After merging with our cybercrime beta (β_{TCCA}) and financial fundamentals, we have 1743 firms in the sample from 2012 to 2021.

We calculate the cumulative average of total IT spending, total assets, and IT/Assets for the lowest (P1) and highest (P5) cybercrime beta stocks from 2013 to 2021. The top panel of Figure 7 shows that low cybercrime beta firms in P1 consistently outspend their P5 counterparts in IT investments, with the disparity widening notably after 2015. The middle panel shows the total assets for firms in P1 and P5.[39] Firms with higher cybercrime risk (P1) also experience more rapid asset growth compared to those better hedged against cybercrime (P5). Importantly, this trend persists even when IT spending is considered relative to total assets, as illustrated in the lower panel, revealing that firms with higher cybercrime risk (P1) dedicate a greater share of their assets to IT investments compared to those more insulated from cybercrime (P5).

These findings are consistent with the implications of the models discussed above. Firms in P1 spend a lot on IT investment to innovate and protect themselves from cyber attacks to sustain growth. Cybercriminals find this valuable data increasingly tempting and the market prices this risk accordingly (Gomes et al., 2023). We posit that, as concerns about cybercrime risk increase, investors value firms that can effectively hedge against cybercrime. Therefore, a low IT/Assets

[36] A recent study by He et al. (2021) uses the same data set to explore the question of IT spending in banking.

[37] For example, ABC company has two IDs because the name of the company is recorded by either ABC Ltd. or ABC Corp.

[38] We manually check matched firms, and the accuracy is about 99% by using 0.67 as the threshold.

[39] We normalize all sub-figures to start from zero for visual presentation. The 2013 value in our figures is cumulative, incorporating data from 2012.

ratio reduces firms' exposure to cybercrime risk (high cybercrime beta) when cybercrime concerns are raised in the market.

We test the importance of the IT/Assets ratio ("IT Budget") during times of heightened cybercrime risk by regressing β_{TCCA} on the interaction term between *HCCR* and IT Budget. The control variables are the same as the digitization investigation in Table 7. All regressors are standardized to have a mean of zero and a standard deviation of one.

Table 8 reports the estimation results. Column (1) shows that the estimated coefficient on the interaction term *HCCR*× IT Budget is negative and significant at the 1% level. The result is essentially unchanged by including control variables in column (2). An decrease in the IT Budget ratio of one within standard deviation, results in a 1.3% increase in the firm's cybercrime beta relative to its own within standard deviation. These results indicate that a firm with a low IT/Assets ratio has a reduced exposure to cybercrime risk during periods of high cybercrime news coverage.

In subsequent columns, we break down the IT Budget into four sub-categories: spending on hardware, software, commutation, and services. Interestingly, with the exception of service spending, the interaction terms between *HCCR* and software is negative and significant at the 1% level; meanwhile, hardware and communication spending are borderline significant. These results indicate that firms spending less on hardware, software, and communication in IT-related investment per given unit of assets, have reduced exposure to cybercrime risk in periods of heightened risk.

The empirical evidence in this section is consistent with the theoretical propositions of a cybercrime-induced innovation feedback loop in the study by Gomes et al. (2023). Firms adopting data-driven business models to drive their growth and innovation need high levels of IT investment (Brynjolfsson and McElheran, 2016). When these investments successfully foster sustainable growth through digital innovation, they not only justify the expenditure but also elevate the value of the firm's data, inadvertently making it a more lucrative target for cybercriminals. Conversely, firms less reliant on data-driven strategies tend to allocate less towards IT for growth or innovation, resulting in lower digital-related and IT expenditures. This lower investment level, while indicative of a business model less dependent on digitization, paradoxically renders these firms less appealing to cybercriminals and potentially more resilient to attacks due to their conservative IT spending.

5 Hedging and Cyber Risk Insurance Costs

We now return to discuss the implications of our earlier asset pricing results for the hedging and insurance of cybercrime risks. This section makes two contributions. We first use our asset pricing results to construct an insurance-like hedging portfolio, and examine its performance across major cyber crime events that have affected the US economy. Having demonstrated the encouraging hedging performance of the portfolio, we turn to the cybercrime risk premium and the implied insurance costs.

On April 17 2022, *The Wall Street Journal* published a news article titled "Insurers Wary of Longer-Term Costs of Cyberattacks", highlighting the difficulties insurance underwriters are facing over cyber insurance cover.[40] As a new species of systematic risk, the lack of historical data and limited awareness of the true cyber risk exposures of business entities mean that insurance companies face challenges in setting the premium and policy coverage limits. Underpricing new products risks insurance company insolvency (Mohey-Deen and Rosen, 2018). Granato et al. (2019) highlight the challenges in estimating insured losses following cyber-related incidents, in part because cyberattacks often affect many organizations simultaneously. A recent survey by Koijen and Yogo (2022) highlights the challenges and difficulties faced by policy issuers in the cyber risk insurance market from an academic point of view. Hence, pricing and designing contracts for cyber risk by referencing other markets with tail or disaster risks is a ripe field for academic research to explore.

[40] https://www.wsj.com/articles/insurers-wary-of-longer-term-costs-of-cyberattacks-3912feaf.

5.1 Evaluation of a cyber hedge strategy

Cybercrime was highlighted as one of the top global risks by the 2021 WEF Global Risk Report (McLennan, 2021).[41] Implementable investing strategies that hedge against climate risk have been discussed in the climate risk literature.[42] Although cybercrime is a systematic risk causing huge economic loss, investors increasingly struggle find cybersecurity insurance. We propose an effective insurance-like portfolio to hedge losses from cyberattacks and examine the performance of this hedging portfolio in an event study analysis.

We collect cyber events recorded by the Center for Strategic & International Studies (CSIS). CSIS records 778 global cyber incidents from 2006 to 2021, of which 519 incidents were reported online within one month. We search Google to find the earliest news report of each incident.[43]

We retain only those incidents related to the US by manually reading news reports or articles, leaving us with 266 US-related incidents between 2007 and 2021, or around 1.5 cyber-related crimes each month. In months with multiple incidents we retain only the first incident, reducing the samople to 112 significant cyber events. Our sample of incidents include notorious cyberattacks such as Citi Bank in 2011, Equifax in 2017, and Colonial Pipeline in 2021.

To validate the cyber incident dates reported data by web crawlers, we inspect if these cyber incidents significantly increase the Refinitiv cybercrime news coverage (*CCB*). We assign a dummy variable equal to 1 for days we find cyber incidents and zero otherwise. Panel A in Table 9 shows cyber incident days coincide with cybercrime news coverage for the 112 incidents.

The hedging portfolio construction is similar to the methodology outlined by Alekseev et al. (2022). At the end of each month, we form five portfolios based on the β_{TCCA} estimated from

[41] The top 10 risks include extreme weather, climate action failure, human environmental damage, infectious diseases, biodiversity loss, digital power concentration, digital inequality, interstate relations fracture, cybersecurity failure, and likelihood crises.

[42] For example, Andersson et al. (2016) propose a strategy by investing in a decarbonized index to hedge climate risk for institutional investors. The seminal study by Engle et al. (2020) constructs mimicking portfolios to hedging against climate news risk innovation.

[43] We carefully handle public information available to investors when incidents happen or are reported in the news during market closing time, weekends, or market closing days, assigning the cyber incident information day to the next trading day. For example, the Equifax cyberattack was released to the public after 5:00 PM on September 7, 2017; we corrected this to September 8, 2017.

equation (7). We then compute the five portfolios' abnormal daily return using a CAPM benchmark model around each event.

Notably, our hedging strategy is implementable since any investor or fund manager can construct the portfolios based on available information up to time t and hold the long-short portfolio for time $t+1$. In other words, investors can form a portfolio that mimics an insurance-like asset at month end, and the insurance-mimicking portfolio hedges risks induced by cyber incidents occurring in following month.

Figure 8 presents the average performance of five portfolios across the 112 cyber incidents in 10 days window. Portfolio 5 underperforms portfolio 1 before the cyber incident day (t_0) because investors pay a higher price for cybercrime hedging assets to accept a lower expected return. However, when a cyber incident becomes public knowledge at t_0, portfolio 5 swiftly demonstrates its hedging power. The red solid line with squares in Figure 8 clearly shows that average cumulative returns in portfolio 5 immediately shift upward and outperform all other portfolios up to five days after the cyber incident. On the contrary, portfolio 1 shown with the blue solid line with circles underperforms after incident. Essentially, the statistical results are shown in Panel B of Table 9. The long-short hedging portfolio earns a highly statistically significant 0.37% in the two-day post-incident window.

A back-of-the-envelope calculation implies a substantial economic gain from our insurance hedging strategy against cyber attacks. The average one-day hedging return from $CAR_{t,t+1}$ is 0.19% (0.37%/2). There are 8 cyber incidents per year based on 112 incidents in the 14 years from 2007 to 2021. The Poisson probability of eight incidents in one year is about 14%.[44] The total market value of stock market in 2022 was \$40.51 trillion. Our hedging portfolio prevents cybercrime-induced systematic loss of \$86.21 billion per year ($0.19\% \times 8 \times 0.14 \times \$40.51 \times 1000$), consistent with the estimated amount of annual loss (\$57 to \$109 billion) by The U.S. Council of Economics Advisers in the 2018 report.

Such hedging portfolios are not easily constructed from methods in the cybercrime literature.

[44] Eight cyber incidents per year implies the Poisson intensity λ=8. Therefore, $P(X=8)=\frac{8^8\times e^{-8}}{8!}\approx 14\%$

The first year in Florackis et al. (2023)'s study is 2007; therefore, we construct three portfolios from the second quarter of 2008 to the first quarter of 2019. Portfolio 1 (P1) contains firms with zero cybersecurity risk exposure from 10-K textual information. Portfolios 2 and 3 are divided based on the median of all non-zero 10-K-based risk measures. The hedging portfolio is long stocks in P1 and short stocks in P3. We evaluate performance across 80 cyber incidents from April 2008 to March 2019.

Figure 9 shows the average performance of three portfolios across 80 cyber incidents with a 10 days window. P1 shows slight outperformance compared to P3 post-incident, but the hedging magnitude is negligible as demonstrated by the results in Table 10. The low-minus-high (LH) hedging portfolio earns statistically insignificant and economically small abnormal returns for all days after these events.

5.2 The cybercrime risk premium and cyber risk insurance implications

Having established the effectiveness of our hedging strategy, we next quantify the risk premium investors pay to hold these cybercrime hedging assets, thereby giving insights into the cyber risk insurance premium from an asset pricing perspective.

We calculate the insurance premium as follows:

$$E(IP) = E(MV_t) * 12 * N_{firms} * E(FCCA_t) \tag{9}$$

where $E(IP)$ is the expected insurance premium that cyber risk insurance underwriters can charge. $E(MV_t)$ is the expected median market value of either all firms (\$821.73 million) in our sample for upper-bound calculation or firms that are more exposed to cybercrime risk in P1 (\$1135.78) for a lower-bound calculation. N_{firms} is the average number of total firms or firms in P1 in our sample, which equals 3257 or 702, respectively. $E(FCCA_t)$ is the expected monthly risk premium as a return-based calculation from the asset pricing model we turn to next.

In deriving the risk premium, we follow Lamont (2001), Ang et al. (2006) and Engle et al.

(2020). From each rolling window one-year regression of equation (5), we estimate the weights, b_t, on returns from each candidate value-weighted traded asset portfolio, Z_t, that track the risk exposure to innovations in the cybercrime news series. Therefore, we have portfolio weights at the end of each portfolio formation period. We then calculate the ex-post pricing factor, $FCCA_{t+1}$, as:

$$FCCA_{t+1} = b_t' \times R_{t+1} \tag{10}$$

where $R_{t+1} = r_{p,t+1}^{\beta_{CCA}}$ is the vector of five portfolio returns in the month following the estimation window. For example, in step 1, we estimate the weights b' using data from 01/01/1998 to 12/31/1998 by using equation (5). We then multiply b' by the vector of returns earned by the five value-weighted portfolio returns in January 1999 to obtain the cybercrime pricing factor return for January 1999. We continue by rolling forward one calendar month, estimating weights over the updated one-year rolling window and multiplying these by returns earned in the subsequent month to obtain the pricing factor return for our full sample through December 2021.[45]

The first column of Table 11 shows that the ex-post cybercrime news shock pricing factor earns -0.44% per month, on average, with an associated t-statistic of 3.51. Subsequent columns show that while this factor's returns are marginally correlated with other benchmark pricing factors, it bears little relation to the returns of other commonly used factors and a large unexplained component remains irrespective of the benchmark factors included in the regressions. Harvey et al. (2016) argue that the usual five percent level is too low a threshold when testing for statistical significance of a new pricing factor because of data mining concerns and the large extant body of research examining the cross-section of expected returns. They suggest that any new factor needs an associated t-statistic greater than three, and so it is comforting to note that the average monthly return of the tracking factor has an associated Newey-West t-statistic of around -3.20.

Plugging this risk premium into equation (10) implies investors give up about 5.28% (12 × 0.44%) per year to invest in stocks in P5 for cybercrime risk hedging. Insurance companies

[45] We also construct the ex-post mimicking pricing factor by following the classical method developed by Fama and French (1993). The result is similar.

writing cyber risk insurance policies can expect to earn a similar amount of return to this market-implied cybercrime risk premium. The upper-bound back-of-the-envelope estimation of the cyber risk premium for the whole stock market is \$141.31 billion (\$821.73 $\times$ 5.28% $\times$ 3257). The lower-bound calculation for the most exposed firms in P1 is \$42.10 billion (\$1135.78 $\times$ 5.28% $\times$ 702). To put these costs in perspective, CEA (2018) estimate annual cyber-related losses that range from \$57 to \$109.

Based on the congressional committees' report by the United States Government Accountability Office, insurance companies have increased the price of cyber risk insurance and lowered coverage limits due to the increased number of cyberattacks and rising insured costs. Although the direct written premium has increased from \$2.1 to \$3.1 billion from 2016 to 2019, this growth implies the coverage limit is less than 6% of the losses estimated by CEA (2018). The insurance industry faces multiple challenges to expand, and some 70% cybersecurity policies are issued by just ten insurance groups in the market (GAO, 2021). Our risk premium estimation provides an initial reference point for insurers, which we leave to be refined in future studies.

6 Robustness Checks

6.1 Google search trend data

The basis of our analysis has been the Refinitiv MarketPsych cybercrime news series, essentially a measure of the supply of information about cybercrime in the press. This section shows that an alternative, publicly-available measure of the demand for information about cybercrime generates very similar results. Specifically, we use daily Google search trend data on the single keyword "cybercrime" from 01/01/2007 to 12/31/2021, an interval considerably shorter than the one used for Refinitiv MarketPsych cybercrime index-based analysis but still long enough to provide meaningful results. We take the first log difference of the Google search trend measure as a measure of investors' demand for cybercrime-related issues.

We estimate the Google cybercrime beta as follows:

$$\Delta SVI_t = \log SVI_t - \log SVI_{t-1}$$

$$R_{i,t} = \alpha_i + \beta_{MKT,i} R_{MKT,t} + \beta_{SVI,i} \Delta SVI_t \tag{11}$$

thus, we conduct the portfolio analysis and contract the ex-ante portfolio tracking factor (denoted by $TSVI$) in the Google Search Trend data universe. Table 12 shows the results are very consistent with the ones in Table 2 using the Refinitiv MarketPsych cybercrime news index. Additionally, we repeat the construction of the ex-post tracking factor. In an untabulated appendix, the results are consistent with the tracking factor created by using news-measured cybercrime risk.

We conclude that our results are not sensitive to considering innovations in the supply of information on cybercrime from the Refinitiv data series, or innovations in the demand for cybercrime information from Google search data. In both cases, hedging stocks that offer better returns when such shocks occur command a high price and hence offer lower returns, on average.

6.2 Alternative pricing factor construction methods

In this sub-section, we demonstrate the insensitivity of our results to constructing the pricing factor using the Fama-French approach, rather than the regression approach detailed in section 5.2. We also continue to demonstrate the consistency of our results when using Google search trend proxies of cybercrime.

Table III in the Online Appendix reports the results of constructing a Fama-French-style pricing factor using estimates of stocks sensitivities to innovations in the Refinitiv series (β_{CCA}). Stocks are sorted into intersections of two portfolios according to market capitalization using NYSE breakpoints and three portfolios according to cybercrime news sensitivities. The factor is then constructed as the average return in the large and small cap high sensitivities portfolios minus the average return in the large and small cap low sensitivities portfolios. The average return on this factor is -0.37% per month with an associated t-statistic of 2.81. The other columns in this panel show that this survives the inclusion of alternative commonly-used factors.

Table IV in the Online Appendix replicates this but uses sensitivities to the Google search trend of cybercrime rather than innovations to Refinitiv's cybercrime news series. The headline results show that the pricing factor is economically large, statistically significant, and is not much affected by accounting for other factors remains. However, compared with both the results in Table III and IV, it is noticeable that several other factors are significantly related to this version of the pricing factor. Nevertheless, including these only serves to increase the magnitude of the pricing factor's alpha.

6.3 Robust to only S&P 500 Stocks

We further investigate if our results are driven by small and illiquid stocks, which are not implementable and suffer data mining issues stressed by Harvey et al. (2016). We re-create Table 2 by only testing stocks from S&P 500. Table V and VI in the Online Appendix shows our key findings also hold in the narrow cross-section of large, liquid, and S&P 500 stocks.

7 Conclusion

We study the influence of firms' sensitivities to cybercrime on the pricing of individual stocks and equity portfolios, utilizing a news-based cybercrime index from Refinitiv MarketPsych and corroborating findings with Google search trends data. Our analysis reveals that stocks with negative beta exposures to innovations in cybercrime news, indicative of a vulnerability to cyber threats, command higher future returns, consistent with the Intertemporal Capital Asset Pricing Model (ICAPM) framework. Conversely, stocks that hedge against cybercrime shocks by covarying positively with cybercrime news innovations yield lower returns.

Bivariate portfolio-level analyses and stock-level cross-sectional regressions, controlling for established pricing factors, confirm a significant negative correlation between cybercrime beta exposures and subsequent stock returns. This underscores the relevance of cybercrime sensitivity as a determinant in asset pricing, beyond traditional pricing factors.

Having demonstrated that cross-sectional differences in sensitivities to cybercrime news have important asset pricing implications, the obvious question is what drives firm sensitivities. Our analysis considers four key factors that contribute to firms' varying sensitivities to cybercrime risk, particularly during times when cybercrime concerns are heightened in the market.

First, we establish a link between high cybercrime beta assets and robust corporate governance, particularly through a talent density channel. This involves quantifying the presence of top management experts with expertise in risk management, governance, and informatics.

Second, we observe that firms with fewer product market peers reporting cybercrime incidents tend to exhibit higher cybercrime beta, suggesting a transmission of cybercrime risk within industries through spillovers.

Third, we demonstrate an inverse relationship between a firm's digitization level and its cybercrime beta, highlighting the increased vulnerability to cyber threats associated with greater digital adoption. This finding underscores the dual-edged nature of digitization, where the pursuit of growth through digital initiatives simultaneously elevates a firm's cyber risk exposure.

Fourth, we delve into the interplay between IT investment and cybercrime risk, drawing on recent literature concerning the data economy. Using detailed firm-specific IT spending data, we show that firms with significant investments in IT – typically data-driven enterprises – enjoy substantial returns in terms of firm growth (and hence high IT/Assets ratios). This success has a dark side, however, because it makes such firms attractive targets to cybercriminals due to their lucrative data assets. On the flip side, companies with a less data-centric focus yet substantial IT investments for protection tend to be less appealing to cybercriminals and are better shielded against cyber threats. Our analysis reveals a pronounced negative correlation between the ratio of IT spending to assets and firms' sensitivities to cybercrime, underscoring the intricate dynamics at play between technological advances, economic incentives, and cybersecurity.

In the third part of our analysis, we consider the hedging and insurance of cybercrime risks. We demonstrate that high cybercrime beta stocks significantly outperform low beta stocks across

112 significant cyber incidents affecting the U.S. economy. This not only illuminates the protective value of certain stocks against cybercrime risks but also offers a perspective on cybercrime risk insurance from an asset pricing viewpoint. We quantify the stock market-implied price of cyber-risk insurance, shedding light on the potential for expansion in the cyber-risk insurance market. This is particularly important in an era of rapid digitization, where the proliferation of digital technologies fuels innovation but also amplifies cyber vulnerabilities, thereby exacerbating the supply-demand imbalance in the cyber insurance market.

References

Aguilar, L. A. (2014). Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus. In *Cyber Risks and the Boardroom conference, New York Stock Exchange*.

Albuquerque, R., Koskinen, Y., and Zhang, C. (2019). Corporate Social Responsibility and Firm Risk: Theory and Empirical Evidence. *Management Science*, 65(10):4451–4469.

Alekseev, G., Giglio, S., Maingi, Q., Selgrad, J., and Stroebel, J. (2022). A Quantity-Based Approach to Constructing Climate Risk Hedge Portfolios. Technical report, National Bureau of Economic Research.

Amihud, Y. (2002). Illiquidity and stock returns: cross-section and time-series effects. *Journal of Financial Markets*, 5(1):31–56.

Andersson, M., Bolton, P., and Samama, F. (2016). Hedging Climate Risk. *Financial Analysts Journal*, 72(3):13–32.

Ang, A., Hodrick, R. J., Xing, Y., and Zhang, X. (2006). The Cross-Section of Volatility and Expected Returns. *The Journal of Finance*, 61(1):259–299.

Ashraf, M. (2022). The Role of Peer Events in Corporate Governance: Evidence from Data Breaches. *The Accounting Review*, 97(2):1–24.

Babina, T., Fedyk, A., He, A., and Hodson, J. (2024). Artificial intelligence, firm growth, and product innovation. *Journal of Financial Economics*, 151:103745.

Bagnoli, M. and Watts, S. G. (2007). Financial Reporting and Supplemental Voluntary Disclosures. *Journal of Accounting Research*, 45(5):885–913.

Bai, J., Philippon, T., and Savov, A. (2016). Have financial markets become more informative? *Journal of Financial Economics*, 122(3):625–654.

Baker, S. R., Bloom, N., and Davis, S. J. (2016). Measuring Economic Policy Uncertainty. *The Quarterly Journal of Economics*, 131(4):1593–1636.

Baker, S. R., Bloom, N., Davis, S. J., and Sammon, M. C. (2021). What Triggers Stock Market Jumps?

Bali, T. G., Brown, S. J., and Tang, Y. (2017). Is economic uncertainty priced in the cross-section of stock returns? *Journal of Financial Economics*, 126(3):471–489.

Barroso, P., Boons, M., and Karehnke, P. (2021). Time-varying state variable risk premia in the ICAPM. *Journal of Financial Economics*, 139(2):428–451.

Bloom, N., Schankerman, M., and Van Reenen, J. (2013). Identifying Technology Spillovers and Product Market Rivalry. *Econometrica*, 81(4):1347–1393.

Bolton, P. and Kacperczyk, M. (2021). Do investors care about carbon risk? *Journal of Financial Economics*, 142(2):517–549.

Breeden, D. T., Gibbons, M. R., and Litzenberger, R. H. (1989). Empirical Tests of the Consumption-Oriented CAPM. *The Journal of Finance*, 44(2):231–262.

Brogaard, J. and Detzel, A. (2015). The Asset-Pricing Implications of Government Economic Policy Uncertainty. *Management Science*, 61(1):3–18.

Brynjolfsson, E. and McElheran, K. (2016). The Rapid Adoption of Data-Driven Decision-Making. *American Economic Review*, 106(5):134–139.

Bybee, L., Kelly, B. T., and Su, Y. (2023). Narrative Asset Pricing: Interpretable Systematic Risk Factors from News Text. *The Review of Financial Studies*, page hhad042.

Campbell, J. Y., Giglio, S., Polk, C., and Turley, R. (2018). An intertemporal CAPM with stochastic volatility. *Journal of Financial Economics*, 128(2):207–233.

Cao, J., Liang, H., and Zhan, X. (2019). Peer Effects of Corporate Social Responsibility. *Management Science*, 65(12):5487–5503.

Cao, S. S., Fang, V. W., and Lei, L. G. (2021). Negative peer disclosure. *Journal of Financial Economics*, 140(3):815–837.

CEA (2018). The Cost of Malicious Cyber Activity to the U.S. Economy. *The Council of Economic Advisers*.

Chen, W. and Srinivasan, S. (2023). Going digital: implications for firm value and performance. *Review of Accounting Studies*, pages 1–47.

Choi, D., Gao, Z., and Jiang, W. (2020). Attention to Global Warming. *The Review of Financial Studies*, 33(3):1112–1145.

Cohen, L. and Frazzini, A. (2008). Economic Links and Predictable Returns. *The Journal of Finance*, 63(4):1977–2011.

Cohen, L. and Lou, D. (2012). Complicated firms. *Journal of Financial Economics*, 104(2):383–400.

CSIS (2018). 2018 Election Security Scorecard. *Center for Strategic and International Studies*.

Diether, K. B., Malloy, C. J., and Scherbina, A. (2002). Differences of Opinion and the Cross Section of Stock Returns. *The Journal of Finance*, 57(5):2113–2141.

Eisenbach, T. M., Kovner, A., and Lee, M. J. (2022). Cyber risk and the U.S. financial system: A pre-mortem analysis. *Journal of Financial Economics*, 145(3):802–826.

Engle, R. F., Giglio, S., Kelly, B., Lee, H., and Stroebel, J. (2020). Hedging Climate Change News. *The Review of Financial Studies*, 33(3):1184–1216.

Fama, E. F. and French, K. R. (1992). The Cross-Section of Expected Stock Returns. *The Journal of Finance*, 47(2):427–465.

Fama, E. F. and French, K. R. (1993). Common risk factors in the returns on stocks and bonds. *Journal of Financial Economics*, 33(1):3–56.

Fama, E. F. and French, K. R. (2015). A five-factor asset pricing model. *Journal of Financial Economics*, 116(1):1–22.

Fama, E. F. and MacBeth, J. D. (1973). Risk, Return, and Equilibrium: Empirical Tests. *Journal of Political Economy*, 81(3):607–636.

Farboodi, M., Mihet, R., Philippon, T., and Veldkamp, L. (2019). Big Data and Firm Dynamics. In *AEA papers and proceedings*, volume 109, pages 38–42. American Economic Association 2014 Broadway, Suite 305, Nashville, TN 37203.

Farboodi, M. and Veldkamp, L. (2021). A Model of the Data Economy. Technical report, National Bureau of Economic Research.

Fisher, A., Martineau, C., and Sheng, J. (2022). Macroeconomic Attention and Announcement Risk Premia. *The Review of Financial Studies*, 35(11):5057–5093.

Florackis, C., Louca, C., Michaely, R., and Weber, M. (2023). Cybersecurity Risk. *The Review of Financial Studies*.

Foucault, T. and Fresard, L. (2014). Learning from peers' stock prices and corporate investment. *Journal of Financial Economics*, 111(3):554–577.

GAO (2021). CYBER INSURANCE Insurers and Policyholders Face Challenges in an Evolving Market. *United States Government Accountability Office*.

Gao, P. and Liang, P. J. (2013). Informational Feedback, Adverse Selection, and Optimal Disclosure Policy. *Journal of Accounting Research*, 51(5):1133–1158.

Garcia, D. (2013). Sentiment during Recessions. *The Journal of Finance*, 68(3):1267–1300.

Gentzkow, M., Kelly, B., and Taddy, M. (2019). Text as Data. *Journal of Economic Literature*, 57(3):535–74.

Giglio, S. and Xiu, D. (2021). Asset Pricing with Omitted Factors. *Journal of Political Economy*, 129(7):1947–1990.

Gomes, O., Mihet, R., and Rishabh, K. (2023). Growth and Innovation in the Modern Data Economy. *Available at SSRN*.

Granato, A., Polacek, A., et al. (2019). The Growth and Challenges of Cyber Insurance. *Chicago Fed Letter*, 426:1–6.

Harvey, C. R., Liu, Y., and Zhu, H. (2016). … and the Cross-Section of Expected Returns. *The Review of Financial Studies*, 29(1):5–68.

He, Z., Jiang, S., Xu, D., and Yin, X. (2021). Investing in Lending Technology: IT Spending in Banking. *University of Chicago, Becker Friedman Institute for Economics Working Paper*, (2021-116).

Hoberg, G. and Phillips, G. (2016). Text-Based Network Industries and Endogenous Product Differentiation. *Journal of Political Economy*, 124(5):1423–1465.

Hou, K. (2007). Industry Information Diffusion and the Lead-lag Effect in Stock Returns. *The Review of Financial Studies*, 20(4):1113–1138.

Hou, K., Xue, C., and Zhang, L. (2015). Digesting Anomalies: An Investment Approach. *The Review of Financial Studies*, 28(3):650–705.

Hsu, P.-H., Li, K., and Tsou, C.-Y. (2022). The Pollution Premium. *The Journal of Finance, Forthcoming*.

Huberman, G., Kandel, S., and Stambaugh, R. F. (1987). Mimicking Portfolios and Exact Arbitrage Pricing. *The Journal of Finance*, 42(1):1–9.

Huynh, T. D. and Xia, Y. (2021). Climate Change News Risk and Corporate Bond Returns. *Journal of Financial and Quantitative Analysis*, 56(6):1985–2009.

Jamilov, R., Rey, H., and Tahoun, A. (2023). The Anatomy of Cyber Risk. Technical report, National Bureau of Economic Research.

Jegadeesh, N. (1990). Evidence of Predictable Behavior of Security Returns. *The Journal of Finance*, 45(3):881–898.

Jegadeesh, N. and Titman, S. (1993). Returns to Buying Winners and Selling Losers: Implications for Stock Market Efficiency. *The Journal of Finance*, 48(1):65–91.

Jiang, H., Khanna, N., Yang, Q., and Zhou, J. (2024). The Cyber Risk Premium. *Management Science*.

Johnson, S., Boone, P., Breach, A., and Friedman, E. (2000). Corporate governance in the Asian financial crisis. *Journal of Financial Economics*, 58(1-2):141–186.

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

Ke, Z. T., Kelly, B. T., and Xiu, D. (2019). Predicting Returns With Text Data.

Kelly, B., Manela, A., and Moreira, A. (2021). Text Selection. *Journal of Business & Economic Statistics*, 39(4):859–879.

Koijen, R. S. and Yogo, M. (2022). New Perspectives on Insurance. *The Review of Financial Studies*, 35(12):5275–5286.

Kothari, S. P., Shu, S., and Wysocki, P. D. (2009). Do Managers Withhold Bad News? *Journal of Accounting Research*, 47(1):241–276.

Krueger, P., Sautner, Z., and Starks, L. T. (2020). The Importance of Climate Risks for Institutional Investors. *The Review of Financial Studies*, 33(3):1067–1111.

Lamont, O. A. (2001). Economic tracking portfolios. *Journal of Econometrics*, 105(1):161–184.

Larcker, D. F. and Richardson, S. A. (2004). Fees Paid to Audit Firms, Accrual Choices, and Corporate Governance. *Journal of Accounting Research*, 42(3):625–658.

Lee, C. M., Ma, P., and Wang, C. C. (2015). Search-based peer firms: Aggregating investor perceptions through internet co-searches. *Journal of Financial Economics*, 116(2):410–431.

Lins, K. V., Servaes, H., and Tamayo, A. (2017). Social Capital, Trust, and Firm Performance: The Value of Corporate Social Responsibility during the Financial Crisis. *The Journal of Finance*, 72(4):1785–1824.

Liu, J., Moskowitz, T. J., and Stambaugh, R. F. (2021). Pricing Without Mispricing. Technical report, National Bureau of Economic Research.

Liu, Z. and Winegar, A. (2023). Economic Magnitudes Within Reason. *Available at SSRN 4223412*.

Loughran, T. and McDonald, B. (2016). Textual Analysis in Accounting and Finance: A Survey. *Journal of Accounting Research*, 54(4):1187–1230.

Loughran, T. and McDonald, B. (2020). Textual Analysis in Finance. *Annual Review of Financial Economics*, 12:357–375.

McLennan, M. (2021). The Global Risks Report 2021 16th Edition. World Economic Forum Cologny, Switzerland.

Merton, R. C. (1973). AN INTERTEMPORAL CAPITAL ASSET PRICING MODEL. *Econometrica: Journal of the Econometric Society*, pages 867–887.

Mitton, T. (2002). A cross-firm analysis of the impact of corporate governance on the East Asian financial crisis. *Journal of Financial Economics*, 64(2):215–241.

Mitton, T. (2024). Economic Significance in Corporate Finance. *The Review of Corporate Finance Studies*, 13(1):38–79.

Mohey-Deen, Z. and Rosen, R. (2018). The Risks of Pricing New Insurance Products: The Case of Long-Term Care. *Chicago Fed Letter*.

Newey, W. K. and West, K. D. (1987). A Simple, Positive Semi-definite, Heteroskedasticity and Autocorrelation Consistent Covariance Matrix. *Econometrica*, 55(3).

Pedersen, L. H., Fitzgibbons, S., and Pomorski, L. (2021). Responsible investing: The ESG-efficient frontier. *Journal of Financial Economics*, 142(2):572–597.

Peters, G. F. and Romi, A. M. (2013). Discretionary compliance with mandatory environmental disclosures: Evidence from SEC filings. *Journal of Accounting and Public Policy*, 32(4):213–236.

Peterson, R. L. (2016). *Trading on Sentiment: The Power of Minds Over Markets*. John Wiley & Sons.

Shumway, T. (1997). The Delisting Bias in CRSP Data. *The Journal of Finance*, 52(1):327–340.

Sloan, R. G. (1996). Do Stock Prices Fully Reflect Information in Accruals and Cash Flows about Future Earnings? *Accounting Review*, pages 289–315.

Tetlock, P. C. (2007). Giving Content to Investor Sentiment: The Role of Media in the Stock Market. *The Journal of Finance*, 62(3):1139–1168.

Tetlock, P. C. (2015). The Role of Media in Finance. *Handbook of Media Economics*, 1:701–721.

Tseng, K. (2022). Learning from the Joneses: Technology spillover, innovation externality, and stock returns. *Journal of Accounting and Economics*, 73(2-3):101478.

WEF (2022). The Global Risks Report 2022. *World Economic Forum*.

Figure 1: Refinitiv MarketPsych cyberCrime News Index

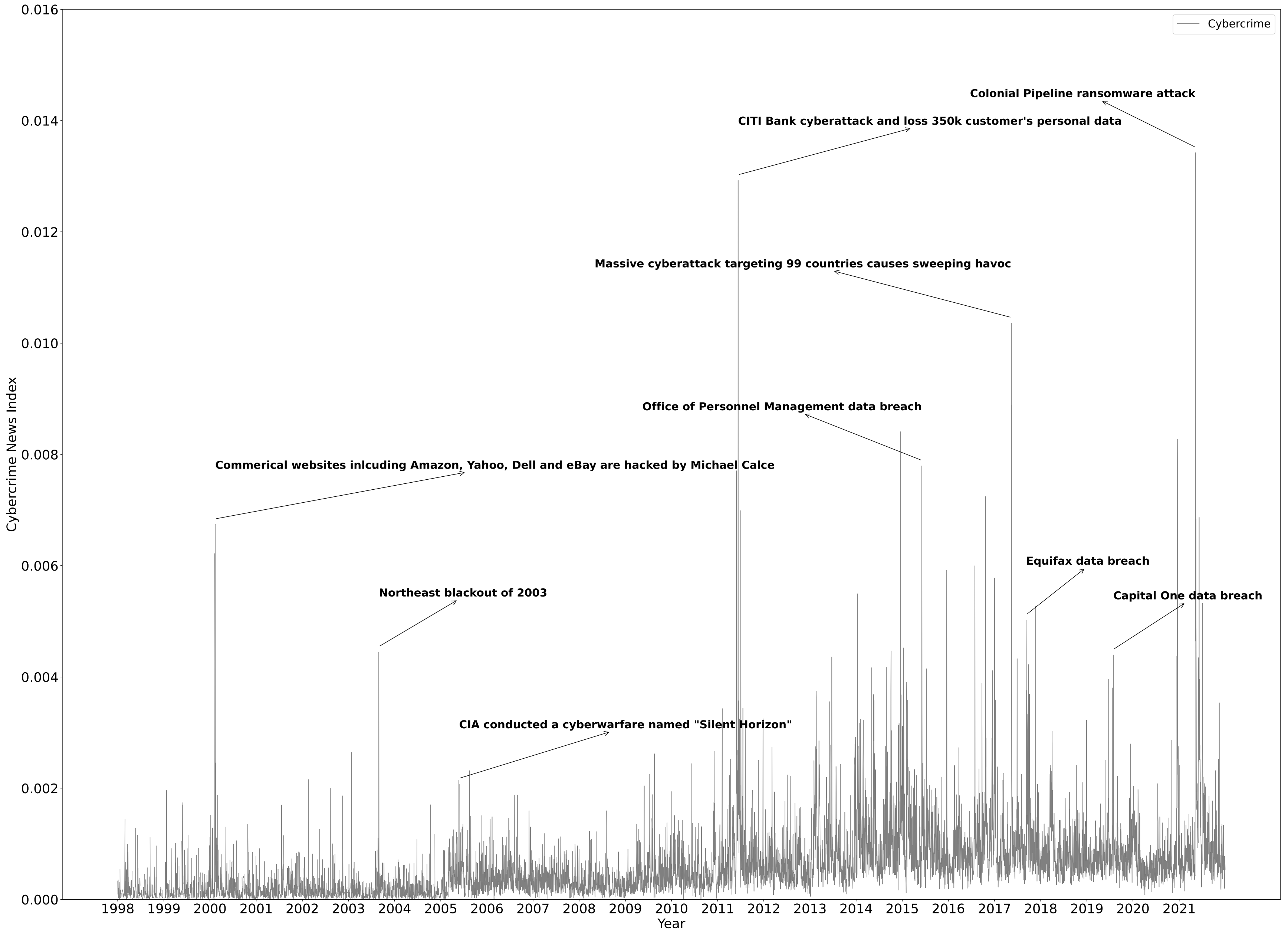

Figure 2: Pearson Correlation between CCA and TCCA in each Rolling Sample Period

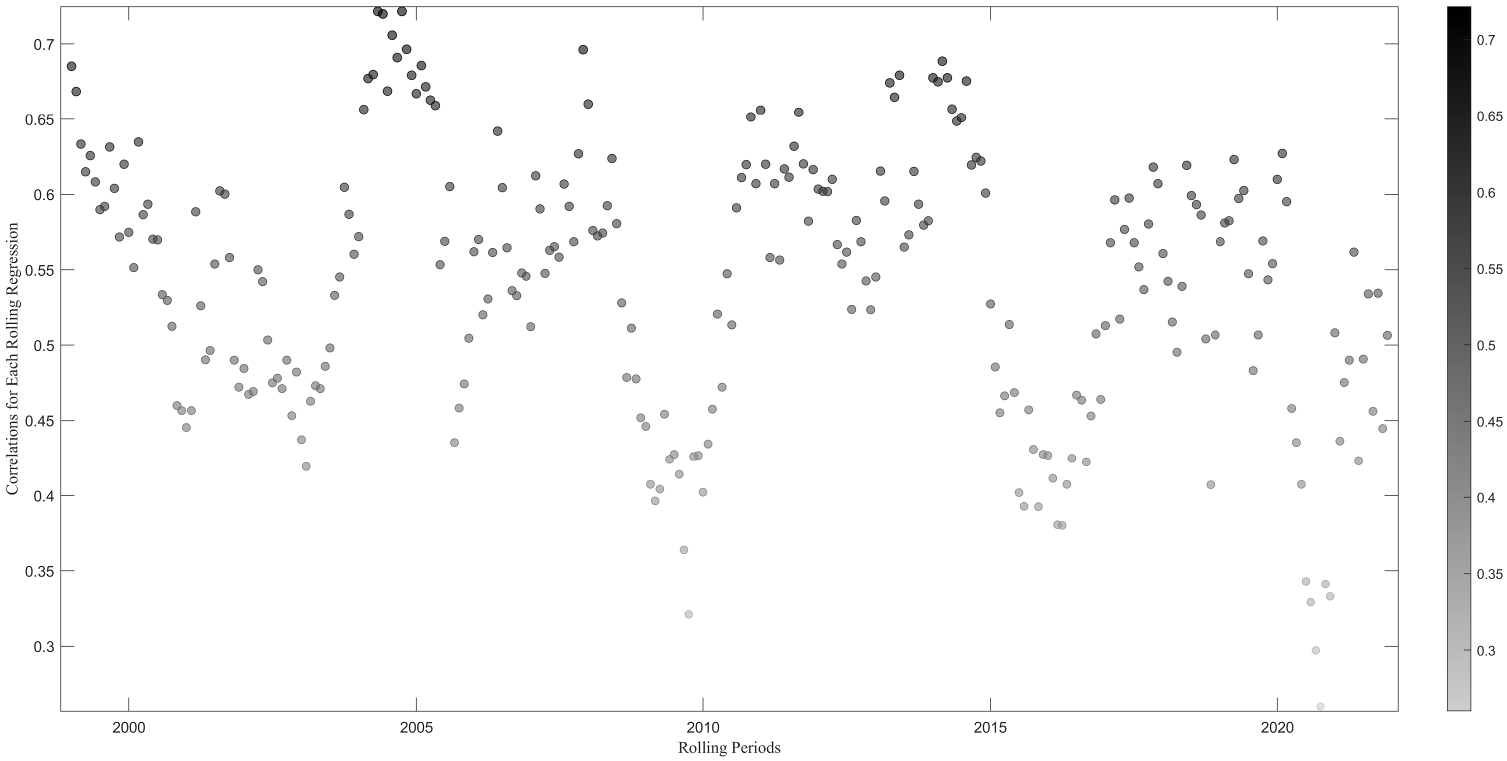

Figure 3: Time-Varying Weights for the Base Assets Formed by β_{CCA}

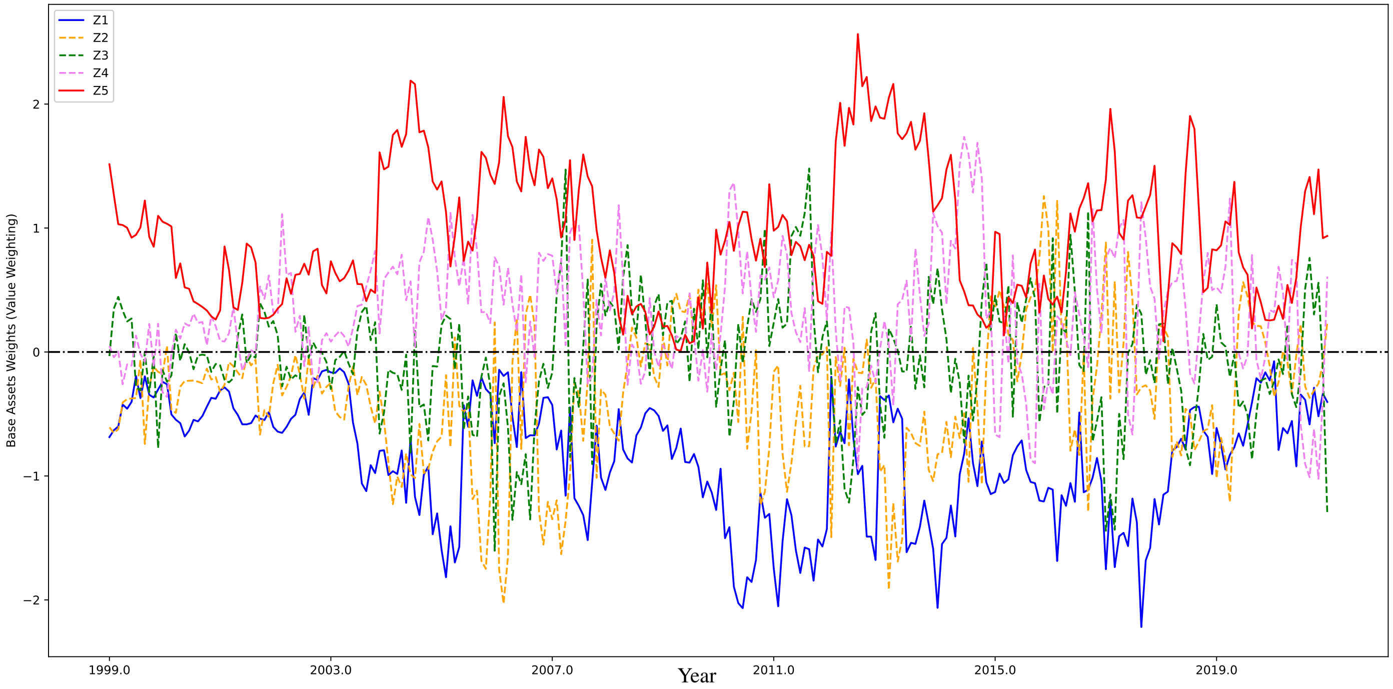

Figure 4: Heatmap of Monthly Cybercrime News Coverage Exceeding 90-Day Moving Average

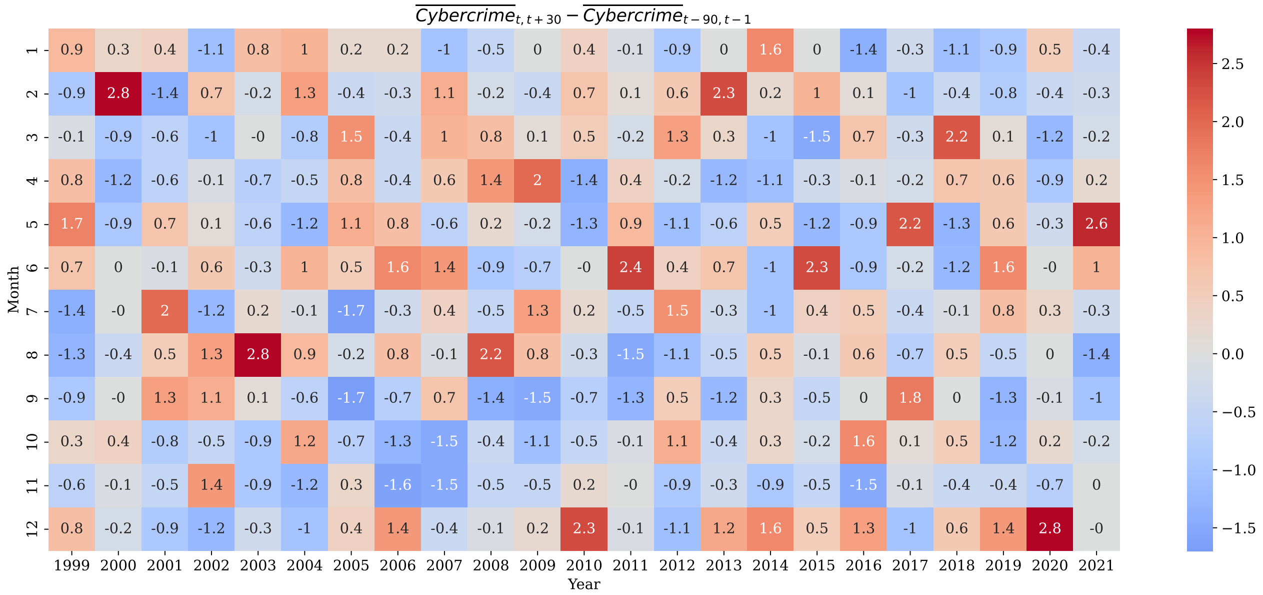

Figure 5: Firm-Level Cybercrime Index from 1998 to 2021

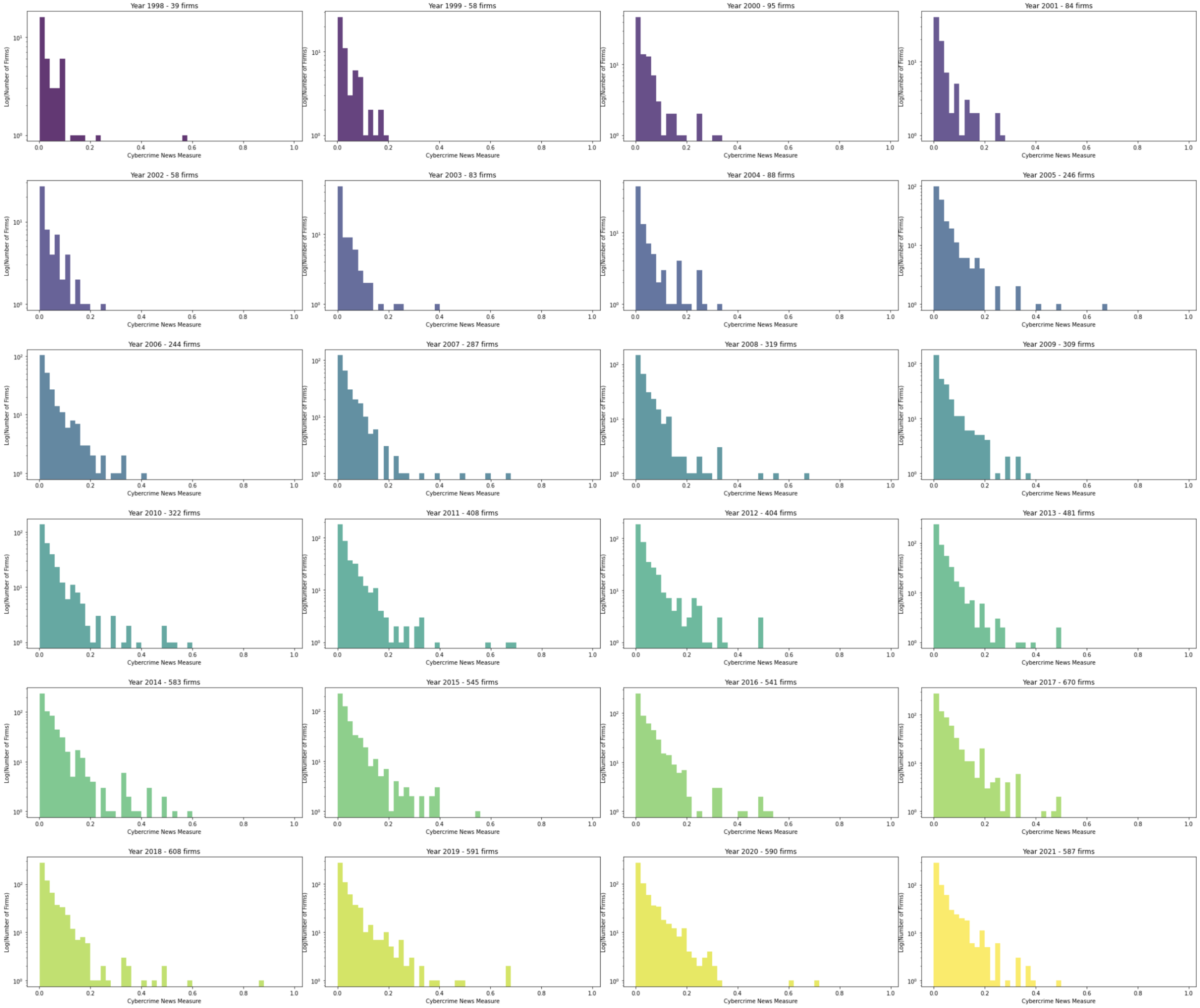

Figure 6: Keywords of Digital Activities in Conference Call

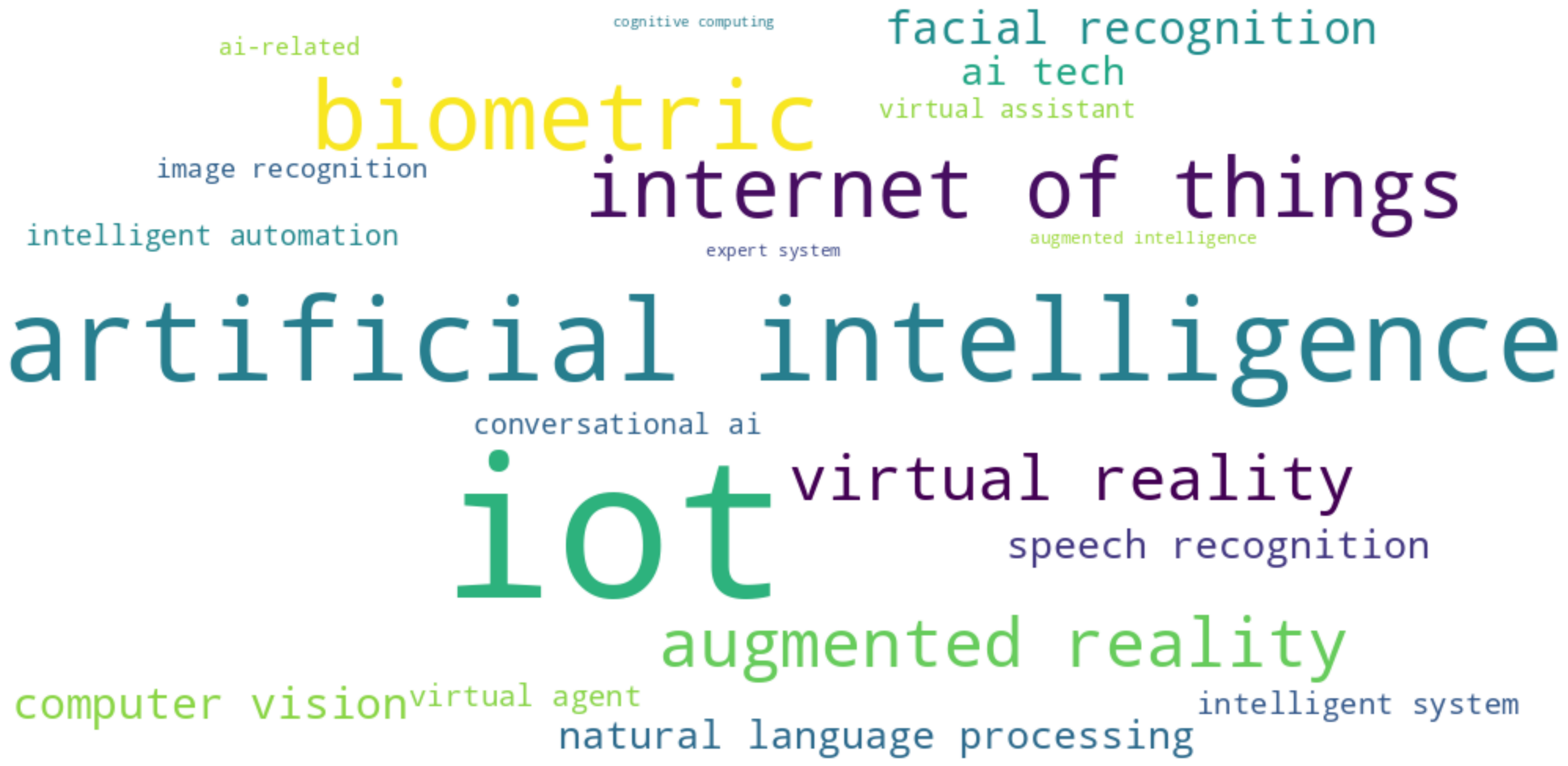

Figure 7: Firms IT Expenditures & Assets P1 and P5 Portfolios from 2013 to 2021

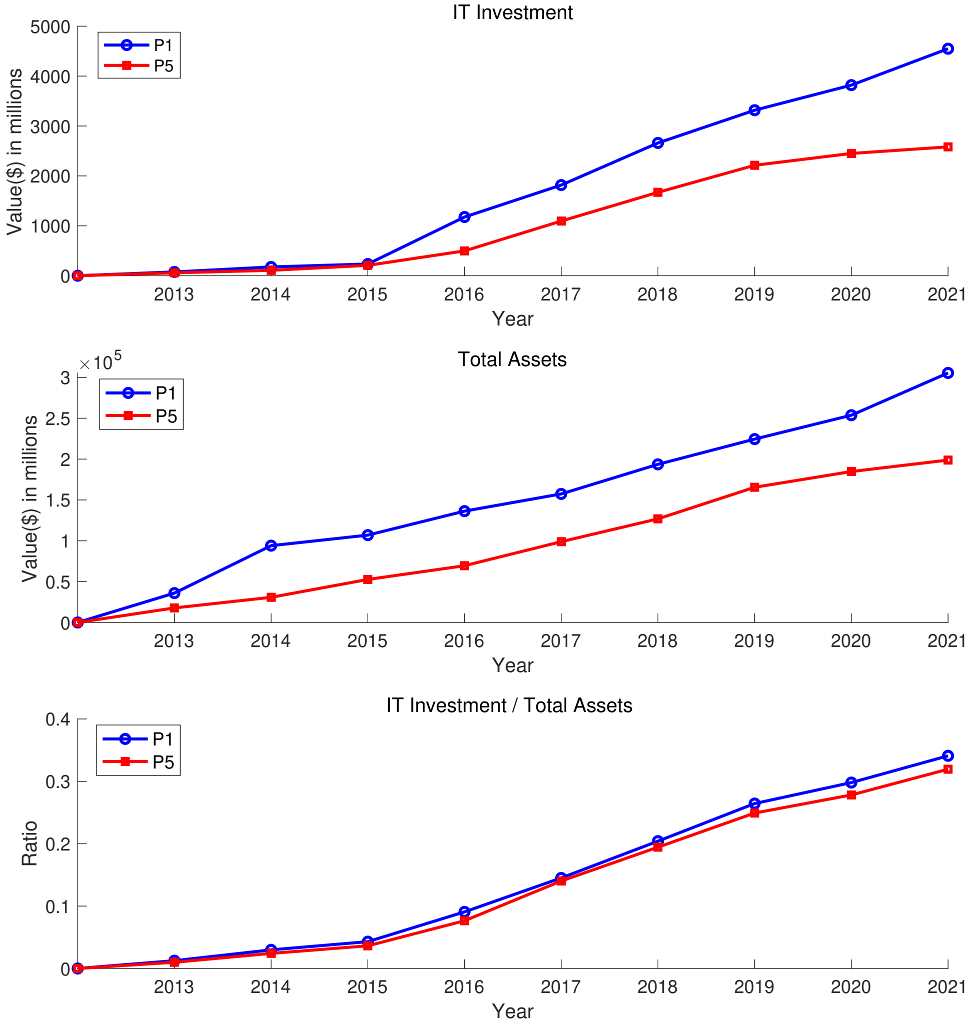

Figure 8: Average Cumulative Abnormal Return in Five Portfolios across 112 Cyber Incidents

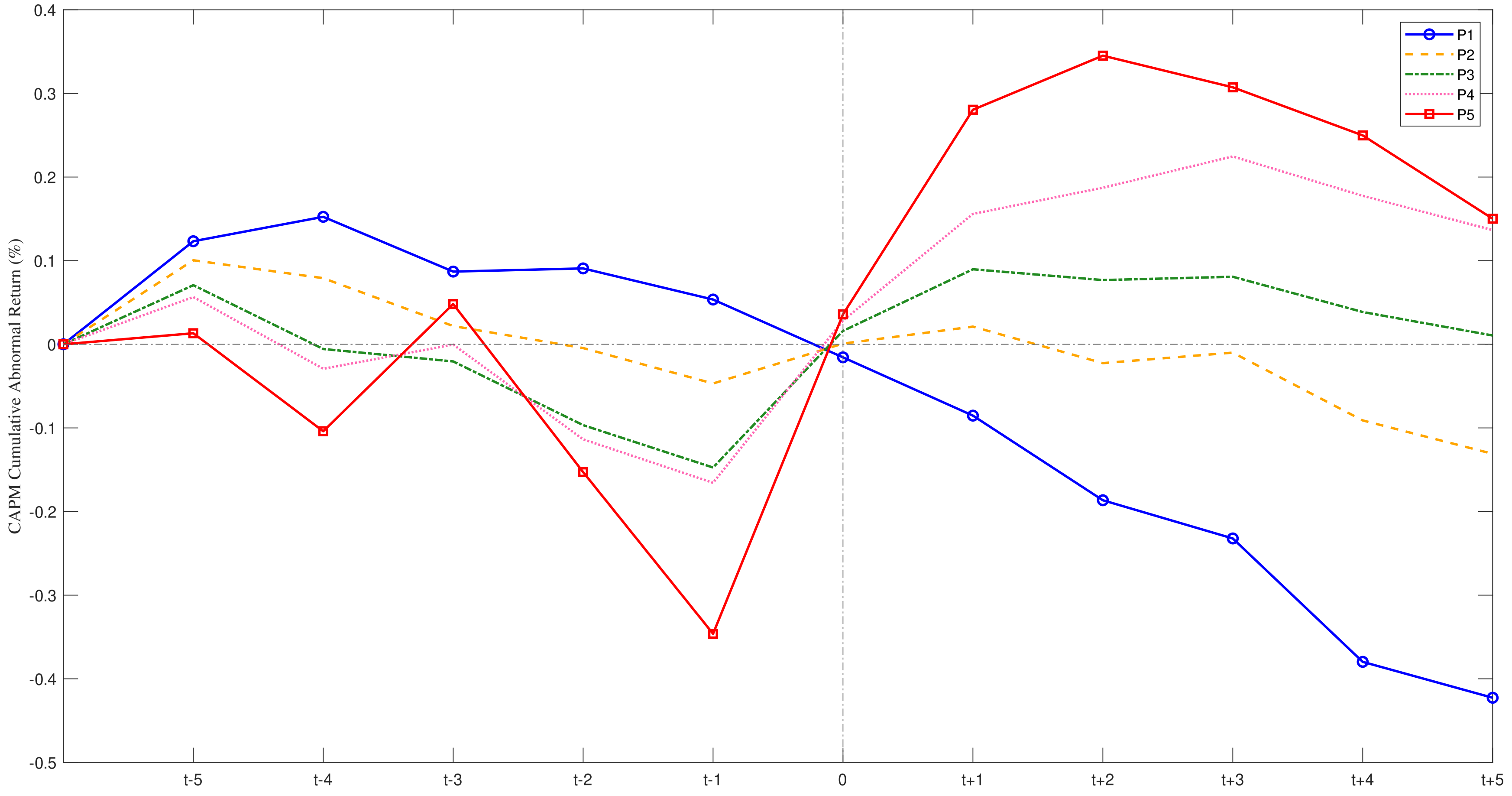

Figure 9: ACAR in Florackis et al. (2023) Portfolios across 80 Cyber Incidents

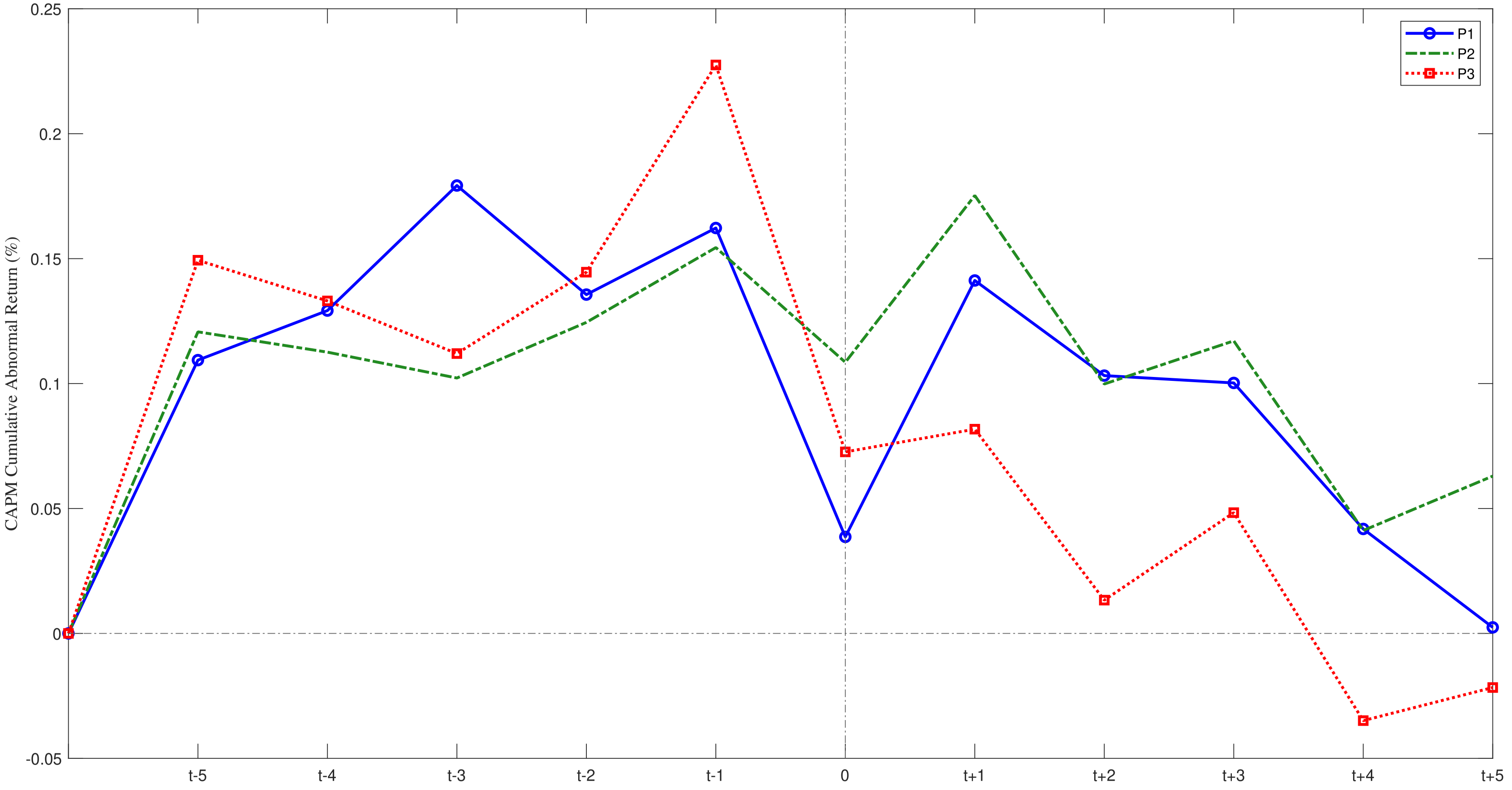

Table 1: AR(6) Coefficients of Refinitiv MarketPschy cyberCrime news measure

This table reports the results from equation (2), an AR(6) model. The left panel presents the autocorrelation coefficients subject to 6 lags. The right panel presents results by adding ΔVIX and ΔEPU as additional control variables. Dicker-Fuller test statistics and innovation AR(1) coefficients are reported for the AR(6) model. The original sample is from 1998:01 to 2021:12, and observations are lost in the right panel subject to the data availability of VIX and EPU. For each regression, the estimated coefficients are reported in line 1, and Newey-West t-statistics are reported in parentheses and computed with 6 lags. N is the number of observations in each regression and $\bar{R}$ is the Adjusted R-squared.

Cybercrime Coverage	CCB_t	CCB_t
CCB_{t-1}	0.68	0.63
	(14.05)	(11.69)
CCB_{t-2}	-0.09	0.06
	(-2.52)	(1.14)
CCB_{t-3}	0.06	0.09
	(1.65)	(1.78)
CCB_{t-4}	0.01	0.07
	(0.29)	(0.98)
CCB_{t-5}	-0.03	0.11
	(-1.05)	(2.61)
CCB_{t-6}	0.23	0.11
	(6.65)	(4.24)
ΔVIX		0.93
		(0.66)
ΔEPU		-0.01
		(-0.26)
DF	-10.35	
Innovation AR(1)	-0.03	
N	8300.00	7206.00
$\bar{R}$	0.58	0.67

Table 2: Portfolio Analysis of Stocks Sorted by β_{TCCA}

This table reports portfolio sorting tests for estimated stock cybercrime beta. Panel A is univariate portfolio sorting based on the β_{TCCA}. First, for each month from December 1998, we form quintile portfolios every month by using NYSE breakpoints, β_{TCCA} is estimated from equation (7), using the last 12 months daily data. Second, we calculate the value-weighted returns for the next month. The first column in Panel A reports individual stocks' average cybercrime tracking beta in each relative beta quintile. The remaining columns in this panel present the average excess returns (RET-RF) and risk-adjusted returns (α_3,α_5,α_6, and α_8) for the quintile value-weighted portfolios and the high minus low portfolio in the last row. α_3 is estimated from Fama and French (1993)) three-factor model; α_5 is estimated from Fama and French (2015) five-factor model; α_6 is estimated from Fama and French (2015) five-factor model augmented with the momentum factor; α_8 is estimated from Fama and French (2015) five-factor model augmented with the momentum, short-term and long-term reversal factor. Panel B presents bivariate portfolio sorting results. First, we sort stocks based on each control variable into quintiles. Second, stocks within each control variable are sorted into quintiles based on β_{TCCA}. The next month's value-weighted portfolio return alphas (α^8) are reported for each β_{TCCA} quintile, averaged across the five control groups. The control variables include firm size (SIZE) measured by market capitalization in millions of dollars, book-to-market ratio (BM), operating profitability (OP), investment (I/A), market beta (β_{MKT}), market volatility beta (β_{VIX}), economic policy uncertainty beta (β_{EPU}), momentum (MOM), last month return (LRET), illiquidity (ILLIQ), idiosyncratic volatility (IVOL), and analyst forecast dispersion (DISP). The differences in $\alpha_8$between quintile 5 (High) and quintile 1 (Low) are presented in the last row. Newey-West adjusted t-statistics are reported in parentheses. The sample period is from 01/01/1998 to 12/31/2021.

Panel A: Univariate Portfolios Sorted by β_{TCCA}

	β_{TCCA}	Excess Return	α_3	α_5	α_6	α_8
Low	-0.66	1.08	0.41	0.40	0.39	0.39
		(3.70)	(2.80)	(2.85)	(2.85)	(2.75)
2	-0.14	0.83	0.25	0.14	0.14	0.11
		(3.19)	(2.64)	(1.72)	(1.63)	(1.38)
3	0.09	0.65	0.06	-0.06	-0.05	-0.07
		(2.35)	(0.81)	(-0.76)	(-0.68)	(-0.96)
4	0.30	0.69	0.04	-0.04	-0.03	-0.03
		(2.37)	(0.42)	(-0.46)	(-0.30)	(-0.27)
High	0.81	0.14	-0.69	-0.53	-0.50	-0.48
		(0.32)	(-3.49)	(-2.92)	(-2.94)	(-2.64)
High-Low		-0.95	-1.09	-0.92	-0.88	-0.86
		(-2.93)	(-3.44)	(-3.12)	(-3.17)	(-2.90)

Panel B: α_8 in Bivariate Portfolios Sorted by β_{TCCA}

β_{TCCA}	SIZE	BM	OP	I/A	β_{MKT}	β_{VIX}	β_{EPU}	MOM	LRET	ILLIQ	IVOL	DISP
Low	0.32	0.36	0.49	0.43	0.32	0.44	0.34	0.37	0.38	0.33	0.36	0.49
	(1.93)	(2.25)	(2.53)	(2.45)	(2.12)	(2.75)	(2.05)	(2.75)	(2.38)	(2.03)	(2.11)	(2.79)
P_2	0.05	0.12	0.05	0.10	0.10	0.05	0.08	0.16	0.04	0.03	0.04	0.07
	(0.68)	(1.51)	(0.51)	(1.22)	(0.99)	(0.58)	(1.04)	(1.85)	(0.54)	(0.43)	(0.45)	(0.90)
P_3	-0.04	0.05	-0.04	-0.04	0.05	-0.06	-0.05	-0.08	-0.02	-0.02	-0.03	-0.05
	(-0.51)	(0.57)	(-0.52)	(-0.46)	(0.71)	(-0.84)	(-0.65)	(-0.98)	(-0.19)	(-0.26)	(-0.29)	(-0.67)
P_4	-0.12	-0.10	-0.11	-0.11	-0.22	-0.15	-0.10	-0.14	-0.15	-0.14	-0.17	-0.13
	(-1.66)	(-1.15)	(-1.16)	(-1.20)	(-2.62)	(-1.67)	(-1.03)	(-1.43)	(-1.68)	(-1.82)	(-1.70)	(-1.30)
High	-0.36	-0.45	-0.45	-0.37	-0.44	-0.44	-0.44	-0.34	-0.41	-0.40	-0.37	-0.37
	(-2.40)	(-2.62)	(-2.74)	(-2.20)	(-2.68)	(-2.60)	(-2.74)	(-2.22)	(-2.52)	(-2.49)	(-2.07)	(-2.63)
High-Low	-0.67	-0.82	-0.93	-0.80	-0.76	-0.87	-0.78	-0.70	-0.79	-0.72	-0.73	-0.87
	(-2.35)	(-2.68)	(-2.84)	(-2.51)	(-2.91)	(-2.93)	(-2.60)	(-2.77)	(-2.70)	(-2.42)	(-2.35)	(-2.94)

Table 3: Stock-Level Fama-MacBeth Cross-Sectional Regressions on β_{TCCA}

This table reports the time-series averages of the slope coefficients from regressing stock one month ahead of excess returns (in percentage) on the cybercrime tracking beta (β_{TCCA}) and a set of control variables with return predictability using Fama-Macbeth cross-sectional regressions. The control variables include firm size (SIZE) measured by the market capitalization in millions of dollars, book-to-market ratio (BM), operating profitability (OP), investment (I/A), market beta (β_{MKT}), market volatility beta (β_{VIX}), economic policy uncertainty beta (β_{EPU}), momentum (MOM), last month return (LRET), illiquidity (ILLIQ), idiosyncratic volatility (IVOL), and analyst forecast dispersion (DISP). $D_{nontech}$ is a dummy variable assigned to 1 if the firms are in the defined non-tech industry and 0 otherwise based on the SIC, NAICS, and GICS codes. The second-column, third-column, and fourth-column report results for controlling different variables. Newey-West adjusted t-statistics are given in parentheses.

	R_{t+1}					
	(1)	(2)	(3)	(4)	(5)	(6)
β_{TCCA}	-0.46	-0.35	-0.27	-0.27	-0.00	0.06
	(-2.62)	(-2.66)	(-2.30)	(-2.15)	(-0.02)	(0.46)
$D_{nontech} \times \beta_{TCCA}$					-0.46	-0.36
					(-2.27)	(-2.34)
$D_{nontech}$					-0.49	-0.32
					(-2.42)	(-1.78)
β_{MKT}		0.02	0.13	0.09	0.00	0.04
		(0.09)	(0.50)	(0.42)	(0.02)	(0.23)
β_{VIX}		-0.07	-0.07	-0.09	-0.08	-0.08
		(-1.25)	(-1.35)	(-1.72)	(-1.64)	(-1.61)
β_{EPU}		-0.19	-0.25	-0.13	-0.15	-0.08
		(-1.01)	(-1.33)	(-0.66)	(-0.84)	(-0.52)
SIZE			-0.03	-0.13	-0.11	-0.08
			(-0.56)	(-1.39)	(-1.20)	(-0.94)
BM			0.04	-0.01	0.05	0.08
			(0.37)	(-0.11)	(0.71)	(1.12)
OP			0.13	0.14	0.16	0.14
			(2.94)	(2.41)	(2.94)	(3.14)
I/A			-0.18	-0.20	-0.20	-0.20
			(-2.61)	(-3.00)	(-3.31)	(-3.47)
Illiquidity				-0.04	-0.03	-0.01
				(-0.66)	(-0.51)	(-0.23)
Reversal				-1.37	-1.45	-1.56
				(-3.40)	(-3.75)	(-4.33)
IVOL				-0.47	-0.74	-0.80
				(-0.94)	(-1.56)	(-1.73)
MOM				0.05	0.08	0.07
				(0.27)	(0.41)	(0.36)
DISP				-0.08	-0.09	-0.09
				(-2.51)	(-2.74)	(-2.86)
Intercept	0.76	0.77	0.92	1.41	1.85	1.69
	(2.24)	(3.33)	(2.16)	(3.15)	(4.54)	(4.22)
FF 12 Industry Control	No	No	No	No	No	Yes
Observations	731,291	731,268	673,529	586,236	586,236	586,236
R-squared	0.02	0.05	0.06	0.09	0.10	0.12

Table 4: β_{TCCA} Estimated by 349 Portfolios with FF5 model

Thie table reports univariate portfolio sorting based on the β_{TCCA} that is estimated with 349 equity portfolios. First, for each of the 49 industry portfolios and 100 portfolios (10× 10 bivariate) formed on size and book-to-market, size and investment, and size and profitability, we estimate the cybercrime tracking beta by using the ex-ante tracking factor ($TCCA$) with Fama and French (2015) five-factor model. Second, we form quintile portfolios from January 1999 to December 2021. The first column reports the equity portfolio's average cybercrime tracking beta in each relative beta quintile. The remaining columns in the panel present the average portfolio excess returns (RET-RF) and risk-adjusted returns (α_5,α_6, and α_8) for the quintile value-weighted portfolios and the high minus low portfolio in the last row. α_5 is estimated from Fama and French (2015) five-factor model; α_6 is estimated from Fama and French (2015) five-factor model augmented with the momentum factor; α_8 is estimated from Fama and French (2015) five-factor model augmented with the momentum, short-term and long-term reversal factor. α_q is estimated from Hou et al. (2015) q-factor model. Newey-West adjusted t-statistics are reported in parentheses.

	β_{TCCA}	Excess Return	α_5	α_6	α_8	α_q
Low	-0.24	0.73	0.09	0.08	0.07	0.03
		(2.34)	(0.97)	(0.88)	(0.74)	(0.35)
P_2	-0.07	0.65	-0.03	-0.02	-0.03	-0.05
		(2.32)	(-0.51)	(-0.38)	(-0.55)	(-0.83)
P_3	0.008	0.67	-0.04	-0.02	-0.03	-0.02
		(2.38)	(-0.62)	(-0.41)	(-0.49)	(-0.24)
P_4	0.09	0.70	-0.02	-0.01	-0.02	0.002
		(2.46)	(-0.28)	(-0.19)	(-0.30)	(0.03)
High	0.27	0.43	-0.17	-0.17	-0.16	-0.23
		(1.41)	(-2.22)	(-2.21)	(-2.16)	(-2.65)
High-Low		-0.30	-0.26	-0.25	-0.23	-0.26
		(-2.68)	(-2.30)	(-2.22)	(-2.05)	(-2.23)

Table 5: β_{TCCA} and Corporate Governance Relationship

This table reports the results from panel regressions of β_{TCCA} on the number of corporate governance measures with additional controls on stock-level characteristics and firm financial variables. First, following the study by Pedersen et al. (2021), we use negated accruals (low accruals) to proxy corporate governance, and we measure the accruals as in Sloan (1996). Second, G is the Refinitiv ESG-based governance score, and firms are categorized into low, medium, and high groups. Third, the *Expert* is the log number of committee members who have expertise in risk oversight (R), security (S), governance (G), operation (O), information (I), technology (T), data, (D) and cyber (C)-related experience reported each year. *HCCR* is a dummy variable assigned to a value of one to denote months where the average cybercrime news coverage exceeds this 90-day benchmark. The stock-level characteristic variables include the market beta (β_{MKT}), the market volatility beta (β_{VIX}), the economic policy uncertainty beta (β_{EPU}), the firm size measured by the logarithm of market capitalization, book-to-market ratio (BM), operating profitability (OP), investment (I/A), last month return (LRET), illiquidity (ILLIQ), idiosyncratic volatility (IVOL), and momentum (MOM). Financial control variables include financial leverage (Leverage) and return on assets (ROA). All regressors are lagged for one period. Based on the data availability, the regressions for accruals or experts are from January 1999 or 2003, respectively, to December 2021. *t* statistics are computed using clustered standard errors at the firm level and reported in parentheses.

	(1)	(2)	(3)	(4)	(5)	(6)	(7)
HCCR × Accruals	0.02	0.02					
	(5.77)	(6.34)					
Accruals	-0.01	-0.01					
	(-1.57)	(-1.69)					
HCCR × G			0.02	0.01	0.01		
			(3.06)	(2.57)	(4.40)		
G			0.00	0.01	0.01		
			(0.32)	(1.18)	(2.62)		
HCCR × Expert						0.01	0.01
						(7.31)	(4.52)
Expert						0.02	0.01
						(3.02)	(1.18)
HCCR × Total Expert							0.00
							(1.09)
Total Expert							0.02
							(3.25)
HCCR	0.02	0.02	0.04	0.04	0.01	0.03	0.02
	(11.59)	(11.26)	(4.05)	(3.47)	(1.56)	(18.91)	(16.16)
β_{MKT}		0.07		0.10	0.07		0.07
		(6.25)		(9.23)	(7.13)		(7.14)
SIZE		-0.05		-0.14	-0.09		-0.09
		(-2.65)		(-3.42)	(-4.26)		(-3.92)
BM		0.03		0.06	0.05		0.04
		(4.25)		(4.09)	(6.24)		(5.49)
MOM		-0.00		-0.05	-0.03		-0.03
		(-0.66)		(-3.44)	(-3.61)		(-3.96)
LRET		0.00		-0.00	0.00		0.00
		(0.85)		(-0.10)	(1.14)		(0.70)
IVOL		0.06		0.22	0.07		0.07
		(2.12)		(8.59)	(2.32)		(2.40)
ILLIQ		0.02		0.31	0.07		0.07
		(1.39)		(8.19)	(3.26)		(3.15)
I/A		-0.00		0.03	-0.00		-0.00
		(-4.96)		(0.07)	(-3.02)		(-2.96)
Leverage		0.02		-0.00	0.02		0.02
		(3.44)		(-0.14)	(2.97)		(2.93)
ROA		0.01		0.09	(0.03		0.03
		(1.94)		(4.87)	(3.96)		(4.48)
Firm Fixed Effect	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year Fixed Effect	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Month Fixed Effect	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	557,718	546,042	208,893	198,346	555,348	561,594	528,513
R-squared	0.21	0.21	0.29	0.32	0.24	0.23	0.24

Table 6: β_{TCCA} and Product Similarity

This table reports the results from panel regressions of β_{TCCA} on firms' product similarity based on peer firms' cybercrime news (*PSPC*) with additional controls on stock-level characteristics and firm financial variables. First, the *PSPC* is calculated in equation (8) based on the product similarity measure by Hoberg and Phillips (2016) and Refinitiv MarketPsych's firm-level cybercrime news index report. Second, #*PSPC* is the count of peers within cybercrime news narratives versus the total peer count. *HCCR* is a dummy variable assigned to a value of one to denote months where the average cybercrime news coverage exceeds this 90-day benchmark. The stock-level characteristic variables include the market beta (β_{MKT}), the market volatility beta (β_{VIX}), the economic policy uncertainty beta (β_{EPU}), the firm size measured by the logarithm of market capitalization, book-to-market ratio (BM), operating profitability (OP), investment (I/A), last month return (LRET), illiquidity (ILLIQ), idiosyncratic volatility (IVOL), and momentum (MOM). Financial control variables include financial leverage (Leverage) and return on assets (ROA). The financial control variables include intangible assets (Intangibility), research and development expenditure (R&D), and return on assets (ROA). All regressors are lagged for one period. Based on the data availability, the regressions are from February 1999 to December 2021. t statistics are computed using clustered standard errors at the firm level and reported in parentheses.

	β_{TCCA}							
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
HCCR × PSPC	-0.01		-0.01					
	(-3.19)		(-3.79)					
PSPC	-0.02		-0.01					
	(-5.36)		(-3.27)					
HCCR × Log(PSPC)		-0.01		-0.01				
		(-3.22)		(-3.84)				
Log(PSPC)		-0.02		-0.01				
		(-5.22)		(-3.04)				
HCCR × #PSPC					-0.01		-0.01	
					(-3.00)		(-3.63)	
#PSPC					-0.02		-0.01	
					(-5.69)		(-3.32)	
HCCR × Log(#PSPC)						-0.005		-0.01
						(-2.87)		(-3.55)
Log(#PSPC)						-0.02		-0.01
						(-5.51)		(-3.02)
HCCR	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02
	(14.34)	(14.34)	(14.36)	(14.36)	(14.33)	(14.36)	(14.37)	(14.37)
Intangibility			-0.02	-0.02			-0.02	-0.02
			(-3.12)	(-3.12)			(-3.13)	(-3.14)
R&D			0.01	0.01			0.01	0.01
			(1.93)	(1.93)			(1.93)	(1.93)
ROA			0.02	0.02			0.02	0.02
			(2.68)	(2.68)			(2.69)	(2.69)
Stock-Level Controls	No	No	Yes	Yes	No	No	Yes	Yes
Firm Fixed Effect	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year Fixed Effect	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Month Fixed Effect	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	679,318	679,318	619,546	619,546	679,318	679,318	619,546	619,546
R-squared	0.22	0.22	0.23	0.23	0.22	0.22	0.23	0.23

Table 7: β_{TCCA} and Digitization

This table reports the results from panel regressions of β_{TCCA} on firms' digitization (Digital) with additional controls on stock-level characteristics and firm financial variables. First, the Digital is measured by the methodology of Chen and Srinivasan (2023) from conference call textual data. Second, QDigital is quantization to Digital to mitigate skewness caused by lots of zeros in the early years. *HCCR* is a dummy variable assigned to a value of one to denote months where the average cybercrime news coverage exceeds this 90-day benchmark. The stock-level characteristic variables include the market beta (β_{MKT}), the market volatility beta (β_{VIX}), the economic policy uncertainty beta (β_{EPU}), the firm size measured by the logarithm of market capitalization, book-to-market ratio (BM), operating profitability (OP), investment (I/A), last month return (LRET), illiquidity (ILLIQ), idiosyncratic volatility (IVOL), and momentum (MOM). Financial control variables include financial leverage (Leverage) and return on assets (ROA). The financial control variables include intangible assets (Intangibility), research and development expenditure (R&D), return on assets (ROA), and productivity. All regressors are lagged for one period. Based on the data availability, the regressions are from January 2003 to December 2021. t statistics are computed using clustered standard errors at the firm level and reported in parentheses.

	β_{TCCA}					
	(1)	(2)	(3)	(4)	(5)	(6)
HCCR × Digital	-0.02	-0.02	-0.02			
	(-9.10)	(-8.20)	(-7.86)			
Digital	-0.02	-0.01	-0.01			
	(-4.42)	(-2.55)	(-2.63)			
HCCR × QDigital				-0.04	-0.03	-0.03
				(-8.74)	(-7.94)	(-7.60)
QDigital				-0.02	-0.01	-0.02
				(-4.11)	(-2.38)	(-2.47)
HCCR × Intangibility			-0.01			-0.01
			(-2.67)			(-2.69)
Intangibility		-0.02	-0.01		-0.02	-0.01
		(-1.75)	(-1.44)		(-1.77)	(-1.45)
HCCR	0.03	0.03	0.03	0.04	0.03	0.03
	(16.57)	(13.05)	(13.10)	(17.94)	(14.62)	(14.65)
R&D		0.03	0.03		0.03	0.03
		(3.04)	(3.04)		(3.03)	(3.03)
ROA		0.05	0.05		0.05	0.05
		(4.52)	(4.52)		(4.52)	(4.52)
Productivity		0.01	0.01		0.01	0.01
		(2.07)	(2.07)		(2.07)	(2.07)
Stock-Level Controls	No	Yes	Yes	No	Yes	Yes
Firm Fixed Effect	Yes	Yes	Yes	Yes	Yes	Yes
Year Fixed Effect	Yes	Yes	Yes	Yes	Yes	Yes
Month Fixed Effect	Yes	Yes	Yes	Yes	Yes	Yes
Observations	343,578	325,694	325,694	343,578	325,694	325,694
R-squared	0.23	0.25	0.25	0.23	0.25	0.25

Table 8: β_{TCCA} and IT Investments.

This table reports the empirical results of the firm's IT investment determinants of the cybercrime beta. We use a granular dataset about firms' investments as a refined analysis. All IT spending measures are scaled by total assets. The dependent variable is β_{TCCA}. The IT Budget is the ratio calculated by a firm's total IT investment divided by total assets. Hardware, Software, Communication, and Service are decomposed ratios from the total IT investment. *HCCR* is a dummy variable assigned to a value of one to denote months where the average cybercrime news coverage exceeds this 90-day benchmark. The stock-level characteristic variables include the market beta (β_{MKT}), the market volatility beta (β_{VIX}), the economic policy uncertainty beta (β_{EPU}), the firm size measured by the logarithm of market capitalization, book-to-market ratio (BM), operating profitability (OP), investment (I/A), last month return (LRET), illiquidity (ILLIQ), idiosyncratic volatility (IVOL), and momentum (MOM). Financial control variables include financial leverage (Leverage) and return on assets (ROA). The financial control variables include intangible assets (Intangibility), research and development expenditure (R&D), return on assets (ROA), and productivity. All regressors are lagged for one period. Based on the IT investment data available, the test for IT Budget and other measures covers the period from January 2013 to December 2021. t statistics are computed using clustered standard errors at the firm level and reported in parentheses.

	β_{TCCA}					
	(1)	(2)	(3)	(4)	(5)	(6)
HCCR × IT Budget	-0.01	-0.01				
	(-2.69)	(-2.42)				
IT Budget	0.01	0.00				
	(0.69)	(0.04)				
HCCR × Hardware			-0.01			
			(-1.60)			
Hardware			-0.01			
			(-1.33)			
HCCR × Software				-0.01		
				(-2.71)		
Software				-0.00		
				(-0.31)		
HCCR × Communication					-0.01	
					(-1.60)	
Communication					-0.01	
					(-1.25)	
HCCR × Service						-0.00
						(-1.05)
Service						-0.01
						(-1.03)
HCCR × Intangibility		-0.00	-0.00	-0.00	-0.00	-0.00
		(-0.32)	(-0.36)	(-0.30)	(-0.39)	(-0.40)
Intangibility		0.04	0.04	0.04	0.04	0.04
		(1.24)	(1.25)	(1.24)	(1.26)	(1.27)
HCCR	0.08	0.07	0.07	0.07	0.07	0.07
	(16.13)	(14.44)	(14.34)	(14.35)	(14.31)	(14.07)
ROA		0.13	0.13	0.13	0.13	0.13
		(3.49)	(3.52)	(3.49)	(3.52)	(3.51)
Productivity		0.01	0.01	0.01	0.01	0.01
		(0.73)	(0.72)	(0.73)	(0.73)	(0.73)
R&D		0.05	0.06	0.05	0.06	0.05
		(1.22)	(1.25)	(1.23)	(1.25)	(1.25)
Stock-Level Controls	No	Yes	Yes	Yes	Yes	Yes
Firm Fixed Effect	Yes	Yes	Yes	Yes	Yes	Yes
Year Fixed Effect	Yes	Yes	Yes	Yes	Yes	Yes
Month Fixed Effect	Yes	Yes	Yes	Yes	Yes	Yes
Observations	79,697	74,797	74,797	74,797	74,797	74,797
R-squared	0.34	0.37	0.37	0.37	0.37	0.37

Table 9: Cybercrime News Hedging Portfolio Evaluation

This table presents the performance evaluation of a cybercrime news hedging portfolio with long positive and short negative cybercrime beta stocks across 112 cyber incidents. The 112 cyber incidents are the first cyber-related crimes in each month from 2007 to 2021, recorded by CSIS as significant incidents in the US. Panel A reports the results to validate the positive relationship between the Refinitiv MarketPsych cybercrime news measure and the cyber incidents we use for the hedging performance evaluation. Panel B reports the five and the long-short (HL) portfolios' cumulative abnormal returns estimated by the CAPM in five days after information about cyber incidents was made to the public. Portfolio abnormal return is the average abnormal return of stocks in each portfolio and then cumulates subject to post-event windows. The cumulative abnormal return in Panel B is reported as %. Newey-West adjusted *t*-statistics are reported in parentheses. The sample period is from 01/01/2007 to 12/31/2021 across 112 cyber incidents.

Panel A: Cyber Incidents and Cybercrime News Coverage

	CCB_t	CCB_t
Intercept	308.47	59.23
	(36.41)	(4.90)
$I_{incident=1}$	336.68	275.93
	(4.31)	(4.24)
CCB_{t-1}		0.66
		13.36
CCB_{t-2}		-0.1
		(-2.57)
CCB_{t-3}		0.05
		(1.3)
CCB_{t-4}		0.01
		(0.25)
CCB_{t-5}		-0.04
		(-1.48)
CCB_{t-6}		0.21
		(6.14)
$\bar{R}$	0.02	0.5

Panel B: Average Cumulative Abnormal Return Post Cyber Incidents

	P1	P2	P3	P4	P5	HL
$CAR_{t,t+1}$	-0.09	0.02	0.09	0.16	0.28	0.37
	(-1.27)	(0.41)	(1.25)	(1.59)	(1.71)	(2.04)
$CAR_{t,t+2}$	-0.19	-0.02	0.08	0.19	0.35	0.53
	(-2.19)	(-0.27)	(0.58)	(1.06)	(1.29)	(1.83)
$CAR_{t,t+3}$	-0.23	-0.01	0.08	0.22	0.31	0.54
	(-2.37)	(-0.10)	(0.61)	(1.22)	(1.09)	(1.82)
$CAR_{t,t+4}$	-0.38	-0.09	0.04	0.18	0.25	0.63
	(-3.56)	(-0.83)	(0.27)	(0.95)	(0.86)	(2.20)
$CAR_{t,t+5}$	-0.43	-0.13	0.01	0.14	0.15	0.57
	(-3.89)	(-1.11)	(0.07)	(0.69)	(0.50)	(1.96)

Table 10: Cybersecurity Risk 10-K Measure Hedging Portfolio Evaluation

This table presents the performance evaluation of a low-minus-high hedging portfolio constructed by using cybersecurity risk measure by Florackis et al. (2023). We follow the portfolio construction method as stated in Florackis et al. (2023). The hedging portfolio is to long stocks in P1 with zero cybersecurity risk and short stocks in P3 with the highest cybersecurity risk exposure across 80 cyber incidents from 2008 to 2019 based on the data availability of cybersecurity risk measure. The 80 cyber incidents are the first cyber-related crimes in each month from 2008 to 2019, recorded by CSIS as significant incidents in the US. The table reports the three and the long-short (LH) portfolios' cumulative abnormal returns estimated by the CAPM in five days after information about cyber incidents was made available to the public. Portfolio abnormal return is the average abnormal return of stocks in each portfolio and then cumulates subject to post-event windows. The cumulative abnormal return in this table is reported as %. Newey-West adjusted t-statistics are reported in parentheses. The sample period is from 04/01/2008 to 03/31/2019 across 80 cyber incidents.

	P1	P2	P3	LH
$CAR_{t,t+1}$	0.14	0.18	0.08	0.06
	(1.75)	(2.56)	(1.27)	(0.91)
$CAR_{t,t+2}$	0.10	0.10	0.01	0.09
	(1.09)	(1.27)	(0.18)	(1.41)
$CAR_{t,t+3}$	0.10	0.10	0.01	0.05
	(1.03)	(1.37)	(0.61)	(0.69)
$CAR_{t,t+4}$	0.04	0.04	-0.03	0.08
	(0.34)	(0.42)	(-0.36)	(0.86)
$CAR_{t,t+5}$	0.00	0.06	-0.02	0.02
	(0.02)	(0.62)	(-0.24)	(0.23)

Table 11: Ex-post Cybercrime Mimicking Value-Weighted Pricing Factor

This table reports the results of the ex-post cybercrime mimicking factor pricing test. First, we estimate the weights b' by using equation (5) on a monthly rolling basis. Second, we multiply b' by the vector of one-month ahead base asset returns that are the five value-weighted portfolio returns sorted by β_{CCA} from equation (4) to obtain the cybercrime ex-post pricing factor return from January 1999 to December 2021. The first column is the average return of the ex-post cybercrime tracking factor. The remaining columns present results based on different pricing models. α_{CAPM} is eatimated from the CAPM model. α_3 is estimated from Fama and French (1993)) three-factor model; α_5 is estimated from Fama and French (2015) five-factor model; α_6 is estimated from Fama and French (2015) five-factor model augmented with the momentum factor; α_8 is estimated from Fama and French (2015) five-factor model augmented with the momentum, short-term and long-term reversal factor; α_q is estimated from Hou et al. (2015) q-factor model. Newey-West adjusted t-statistics are reported in parentheses.

	FCCA Monthly Pricing Factor Test							
	Factor	α_{CAPM}	α_3	α_5	α_6	α_8		α_q
Models	-0.44	-0.44	-0.46	-0.47	-0.46	-0.45		-0.42
	(-3.51)	(-3.47)	(-3.60)	(-3.47)	(-3.48)	(-3.30)		(-3.16)
MKT		0.01	-0.005	-0.005	-0.01	-0.03	R_{MKT}	-0.03
		(0.23)	(-0.12)	(-0.12)	(-0.23)	(-0.60)		(-0.54)
SMB			0.09	0.10	0.10	0.06	R_{ME}	0.04
			(1.81)	(1.61)	(1.64)	(0.99)		(0.72)
HML			0.09	0.07	0.07	0.02	R_{IA}	0.07
			(1.85)	(1.25)	(1.06)	(0.26)		(1.12)
RMW				0.02	0.03	0.06	R_{ROE}	-0.10
				(0.35)	(0.41)	(1.01)		(-1.80)
CMA				-0.03	-0.03	-0.09		
				(-0.34)	(-0.30)	(-0.92)		
UMD					-0.014	-0.021		
					(-0.51)	(-0.87)		
ST						0.02		
						(0.50)		
LT						0.15		
						(2.49)		
$\bar{R}^2$		-0.003	0.02	0.02	0.01	0.03		0.02

Table 12: Univariate Portfolios of Stocks Sorted by Google-Search Trend Based Cybercrime Beta

This table reports univariate portfolio sorting based on the β_{SVI} and β_{TSVI} in the left and right panels, respectively. First, for each month from December 2007, we form quintile portfolios every month by using NYSE breakpoints, β_{SVI} is estimated from equation (11), and β_{TSVI} is estimated from equation (7) by replacing $TCCA$ with $TSVI$, using the last 12 months daily data. Noted that the $TSVI$ is constructed as the same procedure with $TCCA$ by using Google Search Trend data. Second, we calculate the value-weighted returns for the next month. The first column in each panel reports individual stocks' average Google search-based cybercrime beta and average Google search-based cybercrime tracking beta in each relative beta quintile. The remaining columns in each panel present the average excess returns (RET-RF) and risk-adjusted returns (α_3,α_5,α_6, and α_8) for the quintile value-weighted portfolios and the high minus low portfolio in the last row. α_3 is estimated from Fama and French (1993)) three-factor model; α_5 is estimated from Fama and French (2015) five-factor model; α_6 is estimated from Fama and French (2015) five-factor model augmented with the momentum factor; α_8 is estimated from Fama and French (2015) five-factor model augmented with the momentum, short-term and long-term reversal factor. Newey-West adjusted t-statistics are reported in parentheses. The sample period is from 01/01/2007 to 12/31/2021.

		SVI Beta						TSVI Beta				
	β^{SVI}	Excess Return	α_3	α_5	α_6	α_8	β^{TSVI}	Excess Return	α_3	α_5	α_6	α_8
Low	-0.58	1.14	0.10	0.15	0.15	0.15	-2.55	1.34	0.29	0.37	0.38	0.36
		(2.43)	(0.92)	(1.40)	(1.46)	(1.40)		(2.33)	(1.41)	(1.99)	(2.09)	(2.11)
2	-0.16	1.06	0.17	0.11	0.11	0.11	-0.93	1.18	0.26	0.23	0.23	0.23
		(2.80)	(2.38)	(1.55)	(1.59)	(1.52)		(2.92)	(2.56)	(2.34)	(2.50)	(2.49)
3	-0.01	0.97	0.10	0.05	0.05	0.04	-0.17	0.92	0.02	-0.00	-0.01	-0.00
		(2.79)	(1.68)	(0.89)	(0.87)	(0.90)		(2.60)	(0.19)	(-0.02)	(-0.01)	(-0.02)
4	0.15	0.83	-0.10	-0.10	-0.10	-0.11	0.55	0.89	-0.06	-0.42	-0.03	-0.03
		(2.35)	(-1.26)	(-1.31)	(-1.33)	(-1.37)		(2.51)	(-0.51)	(-0.26)	(-0.27)	(-0.24)
High	0.59	0.69	-0.49	-0.37	-0.38	-0.38	1.97	0.57	-0.5	-0.42	-0.42	-0.41
		(1.42)	(-2.88)	(-2.25)	(-2.33)	(-2.20)		(1.38)	(-3.01)	(-2.39)	(-2.55)	(-2.38)
High-Low		-0.45	-0.59	-0.53	-0.53	-0.52		-0.76	-0.79	-0.79	-0.78	-0.77
		(-2.04)	(-2.77)	(-2.41)	(-2.55)	(-2.31)		(-2.12)	(-2.45)	(-2.51)	(-2.73)	(-2.63)

Appendix

A Variable definition

Buzz: This measure is the sum of all references from the news in the US over 24 hours. Source: Refinitiv MarketPsych.

Cybercrime: Fraction of total news references and scrutinizing only cybercrime narratives over 24 hours. Source: Refinitiv MarketPsych.

CCB: The measure of news coverage for cybercrime-related narratives and calculated as $BUZZ_t \times Cybercrime_t$. Source: Refinitiv MarketPsych.

VIX: Daily closing value of VIX. Source: Wharton Research Data Services-CBOE Indexes.

EPU: Daily news-based Economic Policy Uncertainty Index. Source: website from the study by Baker et al. (2016)

$\beta_{\mathbf{CAPM}}$: CAPM beta is estimated by the CAPM model with a one-year daily return rolling window.

$\beta_{\mathbf{VIX}}$: Volatility risk beta is estimated by following the study by Ang et al. (2006).

$\beta_{\mathbf{EPU}}$: EPU uncertainty beta is estimated by augmented CAPM model. Each beta estimation is based on a year daily return rolling window. Specifically, we estimate the ε_{EPU} based on the method of Brogaard and Detzel (2015). Then, we standardize ε_{EPU} in each regression period. β_{EPU} is the regression coefficient on the standardized ε_{EPU} controlling for the market factor in CAPM.

ME: Market value of equity in fiscal year closing price times the total share of the equity. Source: Compustat.

Size: Natural log of market value of equity. Source: Compustat.

BM: Book to Market Ratio as defined in Fama and French (1992). We take the natural logarithm of BM in regressions. Source: Compustat.

ILLIQ: Monthly illiquidity measure as per Amihud (2002). We take the natural logarithm of

ILLIQ in regressions. Source: CRSP.

OP: Operating Profitability, as defined in Fama and French (2015). Source: Compustat.

I/A: Investment measure is defined as in Fama and French (2015) study. Source: Compustat.

MOM: Momentum Return Measure is defined as the cumulative return from $t-11$ to the month $t-1$ before the last month t. Source: CRSP.

LRET: Return from the last month to capture the short-term reversal effect. Source: CRSP.

Idiosyncratic Volatility (IVOL): The residual standard error from Fama and French (2015) five factors plus momentum factor pricing model on a daily rolling basis. Each company must have at least 60 observations to run the time-series regression. Sources: CRSP and Kenneth R. French Data Library.

Forecast Dispersion (DISP): The standard deviation of analysts' earnings forecasts in the most recent month before the quarterly earnings announcement and scaled by the stock price. Source: Institutional Brokers Estimate System (I/B/E/S).

Accruals: The value is calculated following Sloan (1996) and Pedersen et al. (2021). We use negated value (low accruals) as the proxy of corporate governance.

G: ESG-based Governance score. Source: Refinitiv Workspace.

Expert: Number of committee members whose committed names, including works with "risk"(R), "security"(S), "governance"(G), "operation"(O), "information"(I), "technology"(T), "data"(D) and "cyber"(C). The tested variable is taken from a natural log for reducing skewness. Source: BoardEx.

Expert%: Ratio of committee members whose committed names, including RSGOITDC keywords, are divided by the total number of committee members. The tested variable is taken from a natural log for reducing skewness. Source: BoardEx.

Digital: The value is calculated following the methodology of Chen and Srinivasan (2023) based on conference call textual data from 2002 to 2021.

QDigital: The quantized Digital is calculated following the methodology of Chen and Srinivasan (2023). Specifically, we cut Digital into four groups. Firms with a zero value of Digital assign a value of 0. Firms with non-zero values of Digital are assigned values of 1,2,3 based on tercile cutoffs.

PSPC: The firm's similarity with its product market peers with cybercrime news narratives reported in the past one-year rolling window is calculated based on the equation (8). The product similarity measure is from Hoberg and Phillips (2016). Source: Hoberg-Phillips Data Library.

IT Budget: The ratio of a firm's total IT investment divided by total assets (IT budget/Assets). Source: HHM and Compustat.

Hardware: The ratio of a firm's hardware IT spending divided by total assets (IT(hardware) budget/Assets). Source: HHM and Compustat.

Software: The ratio of a firm's software IT spending divided by total assets (IT (software) budget/Assets). Source: HHM and Compustat.

Communication: The ratio of a firm's communication IT spending divided by total assets (IT (communication) budget/Assets). Source: HHM and Compustat.

Service: The ratio of a firm's service IT spending divided by total assets (IT (service) budget/Assets). Source: HHM and Compustat.

HCCR: A dummy variable is assigned to a value of one to denote months where the average cybercrime news coverage exceeds this 90-day benchmark.

Intangibility: The ratio of total intangible assets [$intan$] to total assets [at]. Source: Compustat.

R&D: The ratio of R&D expenditures [xrd] to total assets [at]. We replace the missing value for xrd with zeros. Source: Compustat.

ROA: The ratio of operating income before depreciation [$oibdp$] to total assets [at]. Source: Compustat.

Leverage: Total long-term debt [$dltt$] + total current liabibilities [dlc] to total assets [at] Source: Compustat.

Productivity: Total revenue [$revt$] to total employee [emp] Source: Compustat.

SVI: The number of Google search trends on the keyword ”cybercrime”. Source: Google Search Trends Website.

B Cybercrime vs. cybersecurity risk portfolios

Florackis et al. (2023) measure cybersecurity risk using text analysis of firms' 10-K filings. Although this paper provides compelling evidence for a positive risk premium on firms more exposed to cybersecurity risk, their measure may be influenced by issues with disclosure. As noted above, over 50% of companies are assigned cyber risk values of zero in the early years of the Florackis et al. (2023) sample. This may simply be underreporting as managers may not be aware of the true extent of exposure to cyber risk. For example, the models of Gao and Liang (2013) and Bai et al. (2016) begin with the premise that managers are not aware of all dimensions of firm value but that investors may have more expertise about some of them. Informed trades based on such expertise may mean that stock prices are more informative about these risks than disclosures.

The second problem is that disclosure is influenced by managers' choices, even when mandatory (Peters and Romi, 2013). The large accounting literature on this subject that points to the general conclusion that risk disclosure is strategic and subject to biases towards withholding bad news (Bagnoli and Watts, 2007; Kothari et al., 2009). Guidance issued by the SEC resulted in abrupt increases in disclosure of cyber risks, suggesting that disclosure had been less than full before this encouragement was issued. The updated guidance does not appear to have resulted in complete transparency about cyber risks. Jiang et al. (2024) examine firm disclosures after cyber breaches. They show that prior breach experiences and market reactions to cyber breaches affect how firms alter their disclosures, confirming the strategic nature of manager actions.

Our measure trusts in the ability of markets to see through the veil of disclosure, such that stock prices better reflect true risk exposures. This naturally leads to the empirical question of whether our measure captures the cyber risk premium differently – or perhaps even better – than their measure.

We conduct bivariate dependent sorts to compare the performance of the two measures. To alleviate the issue of too many zero risk measures at the start of their sample, we follow the backfill method proposed in their robustness section. We first sort stocks into five portfolios based on the Florackis et al. (2023) 10-K-based measure. Then, within each portfolio, we form quintile portfolios based on β_{TCCA} estimated from equation (7) and report five-factor alphas. Panel A of Table VII shows that dispersion in β_{TCCA} within 10-K-based portfolios adds information. High minus low β_{TCCA} portfolio alphas are each large and negative, statistically significant in three of five cases.

Conversely, sorting first on β_{TCCA} and then on the 10-K-based measure shows no clear pattern. High minus low portfolio alphas flip the sign and are not statistically significant. We conclude that variation in β_{TCCA} captures the alpha-relevant information contained in the 10-K-based measure but not vice versa.

Online Appendix

Table I: Descriptive Statistics

This table presents descriptive statistics for the key variables used in our analysis. Appendix A defines the variables.

	Mean	Std	P1	P50	P99
β_{TCCA}	0.09	0.78	-1.72	0.03	2.86
BMKT	0.99	0.57	-0.09	0.98	2.53
BVIX	0.05	1.23	-3.18	0.02	3.47
BEPU	-0.01	0.23	-0.65	-0.01	0.60
SIZE	6.74	1.84	3.06	6.61	11.56
BM	0.60	0.60	0.02	0.47	2.63
OP	-0.10	93.28	-1.34	0.20	1.75
I/A	0.18	1.04	-0.37	0.07	2.23
MOM	0.23	0.89	-0.68	0.10	3.13
LRET	0.02	0.17	-0.32	0.01	0.51
IVOL	0.41	0.27	0.11	0.35	1.29
ILLIQ	0.28	1.86	0.00	0.00	5.34
DISP	0.16	1.37	0.00	0.03	2.00
ROA	0.07	0.22	-0.77	0.10	0.40
R&D	0.05	0.12	0.00	0.00	0.53
Leverage	0.20	0.20	0.00	0.16	0.78
Intangibility	0.16	0.20	0.00	0.06	0.76
Productivity	0.37	0.68	0.00	0.22	3.81
Accural	-0.02	0.17	-0.14	-0.04	0.58
G	2.00	0.82	1.0	2.00	3.00
Expert	4.22	3.56	0.00	4.00	16.00
TExpert	16.45	9.50	5.00	14.00	51.00
$PSPC$	0.08	0.15	0.00	0.02	0.71
Digital	0.44	3.43	0.00	0.00	9.23
QDigital	0.19	0.63	0.00	0.00	3.00
Total IT Budget	174.26	1489.98	0.00	2.68	3043.11
Hardware Budget	14.05	115.58	0.00	0.53	228.74
Software Budget	46.85	420.59	0.00	0.58	764.88
Communication Budget	11.48	98.89	0.00	0.27	210.46
Service Budget	54.65	432.94	0.00	0.50	996.79

Table II: Portfolio Analysis of Stocks Sorted by β_{CCA}

This table reports portfolio sorting tests for estimated stock cybercrime news beta. The results are based on univariate portfolio sorting based on the β_{CCA}. First, for each month from December 1998, we form quintile portfolios every month by using NYSE breakpoints, β_{CCA} is estimated from equation (4), using the last 12 months daily data. Second, we calculate the value-weighted returns for the next month. The first column in the panel reports individual stocks' average cybercrime news beta and average cybercrime tracking beta in each relative beta quintile. The remaining columns in each panel present the average excess returns (RET-RF) and risk-adjusted returns (α_3,α_5,α_6, and α_8) for the quintile value-weighted portfolios and the high minus low portfolio in the last row. α_3 is estimated from Fama and French (1993)) three-factor model; α_5 is estimated from Fama and French (2015) five-factor model; α_6 is estimated from Fama and French (2015) five-factor model augmented with the momentum factor; α_8 is estimated from Fama and French (2015) five-factor model augmented with the momentum, short-term and long-term reversal factor. Newey-West adjusted t-statistics are reported in parentheses.

	β_{CCA}	Excess Return	α_3	α_5	α_6	α_8
Low	-0.23	0.94	0.23	0.29	0.29	0.27
		(3.06)	(2.19)	(2.56)	(2.56)	(2.28)
P_2	-0.06	0.77	0.19	0.08	0.08	0.07
		(2.90)	(2.69)	(1.27)	(1.23)	(1.14)
P_3	0.001	0.64	0.04	-0.04	-0.04	-0.04
		(2.51)	(0.58)	(-0.62)	(-0.55)	(-0.55)
P_4	0.06	0.52	-0.09	-0.14	-0.13	-0.14
		(1.85)	(-1.41	(-1.92)	(-1.75)	(-1.85)
High	0.23	0.34	-0.41	-0.36	-0.34	-0.35
		(0.87)	(-3.01)	(-2.52)	(-2.49)	(-2.27)
High-Low		-0.60	-0.64	-0.64	-0.63	-0.62
		(-2.66)	(-3.01)	(-2.83)	(-2.90)	(-2.66)

Table III: Fama-French-Style Cybercrime Mimicking Factor Pricing Test

This table reports the cybercrime mimicking factor pricing test results. First, we estimate β_{CCA} by using equation (4) monthly. Second, we follow the factor construction method by Fama and French (1993) to obtain the cybercrime mimicking factor return from January 1999 to December 2021. The first column is the average return of the ex-post FF-style cybercrime tracking factor. The remaining columns present results based on different pricing models. α^{CAPM} is estimated from the CAPM model. The remaining columns present results based on different pricing models. α_{CAPM} is estimated from the CAPM model. α_3 is estimated from Fama and French (1993)) three-factor model; α_5 is estimated from Fama and French (2015) five-factor model; α_6 is estimated from Fama and French (2015) five-factor model augmented with the momentum factor; α_8 is estimated from Fama and French (2015) five-factor model augmented with the momentum, short-term and long-term reversal factor; α_q is estimated from Hou et al. (2015) q-factor model. Newey-West adjusted t-statistics are reported in parentheses.

	Factor	α_{CAPM}	α_3	α_5	α_6	α_8		α_q
Models	-0.37	-0.39	-0.40	-0.38	-0.37	-0.37		-0.34
	(-2.81)	(-2.98)	(-3.02)	(-2.77)	(-2.83)	(-2.65)		-(2.63)
MKT		0.03	0.03	0.02	0.01	0.00	R_{MKT}	0.01
		(0.75)	(0.86)	(0.63)	(0.17)	(-0.09)		(0.16)
SMB			0.00	0.00	0.02	0.01	R_{ME}	-0.06
			(-0.07)	(0.07)	(0.29)	(0.16)		(-0.93)
HML			0.07	0.09	0.07	0.05	RIA	0.07
			(0.95)	(1.51)	(0.97)	(0.73)		(0.65)
RMW				0.01	0.02	0.03	R_{ROE}	-0.12
				(0.15)	(0.28)	(0.36)		(-1.51)
CMA				-0.08	-0.07	-0.06		
				(-0.72)	(-0.59)	(-0.47)		
UMD					-0.05	-0.04		
					(-1.03)	(-1.04)		
ST						0.04		
						(0.68)		
LT						0.01		
						(0.16)		
$\bar{R}^2$		0.00	0.01	0.01	0.01	0.02		0.02

Table IV: Ex-post SVI Cybercrime Mimicking Value-Weighted Pricing Factor

This table reports the results of the ex-post cybercrime mimicking factor pricing test. First, we estimate the weights b' by using equation (5) on a monthly rolling basis. Second, we multiply b' by the vector of one-month ahead base asset returns that are the five value-weighted portfolio returns sorted by β_{SVI} from equation (11) to obtain the Google search-based cybercrime ex-post pricing factor return from January 2008 to December 2021. The first column is the average return of the ex-post cybercrime tracking factor. The remaining columns present results based on different pricing models. The remaining columns present results based on different pricing models. α_{CAPM} is eatimated from the CAPM model. α_3 is estimated from Fama and French (1993)) three-factor model; α_5 is estimated from Fama and French (2015) five-factor model; α_6 is estimated from Fama and French (2015) five-factor model augmented with the momentum factor; α_8 is estimated from Fama and French (2015) five-factor model augmented with the momentum, short-term and long-term reversal factor; α_q is estimated from Hou et al. (2015) q-factor model. Newey-West adjusted t-statistics are reported in parentheses.

	Factor	α_{CAPM}	α_3	α_5	α_6	α_8		α_q
Models	-0.21	-0.23	-0.26	-0.25	-0.25	-0.26		-0.26
	(-2.39)	(-2.41)	(-2.93)	(-2.95)	(-3.03)	(-3.00)		(-2.96)
MKT		0.02	0.04	0.04	0.05	0.05	R_{MKT}	0.04
		(0.62)	(1.42)	(1.38)	(1.75)	(1.68)		(1.44)
SMB			-0.04	-0.05	-0.05	-0.04	R_{ME}	-0.04
			(-1.42)	(-1.40)	(-1.23)	(-0.92)		(-1.13)
HML			-0.09	-0.06	-0.04	-0.03	R_{IA}	-0.08
			(-2.40)	(-1.64)	(-0.95)	(-0.52)		(-1.78)
RMW				-0.02	-0.02	-0.03	R_{ROE}	0.06
				(-0.34)	(-0.30)	(-0.56)		(1.35)
CMA				-0.05	-0.06	-0.04		
				(-0.89)	(-1.14)	(-0.77)		
UMD					0.04	0.04		
					(1.66)	(1.65)		
ST						0.01		
						(0.28)		
LT						-0.04		
						(-0.59)		
$\bar{R}^2$		0.00	0.06	0.06	0.07	0.06		0.02

Table V: Portfolio Analysis of S&P 500 Stocks Sorted by β_{CCA}

This table reports portfolio sorting tests for estimated S&P 500stock cybercrime news beta. The results are based on univariate portfolio sorting based on the β_{CCA}. First, for each month from December 1998, we form quintile portfolios every month by using NYSE breakpoints, β_{CCA} is estimated from equation (4), using the last 12 months daily data. Second, we calculate the value-weighted returns for the next month. The first column in the panel reports individual stocks' average cybercrime news beta in each relative beta quintile. The remaining columns in each panel present the average excess returns (RET-RF) and risk-adjusted returns (α_3,α_5,α_6, and α_8) for the quintile value-weighted portfolios and the high minus low portfolio in the last row. α_3 is estimated from Fama and French (1993)) three-factor model; α_5 is estimated from Fama and French (2015) five-factor model; α_6 is estimated from Fama and French (2015) five-factor model augmented with the momentum factor; α_8 is estimated from Fama and French (2015) five-factor model augmented with the momentum, short-term and long-term reversal factor. Newey-West adjusted t-statistics are reported in parentheses.

	β_{CCA}	Excess Return	α_3	α_5	α_6	α_8
Low	-0.14	0.83	0.19	0.14	0.14	0.13
		(2.91)	(1.69)	(1.38)	(1.39)	(1.26)
P_2	-0.04	0.69	0.17	0.06	0.06	0.06
		(2.86)	(2.21)	(0.79)	(0.87)	(0.82)
P_3	0.001	0.63	0.08	-0.01	-0.00	0.00
		(2.51)	(0.94)	(-0.08)	(-0.02)	(0.03)
P_4	0.05	0.45	-0.12	-0.20	-0.18	-0.20
		(1.62)	(-1.41)	(-2.18)	(-2.07)	(-2.16)
High	0.15	0.24	-0.41	-0.40	-0.38	-0.38
		(0.67)	(-3.34)	(-3.18)	(-3.07)	(-2.83)
High-Low		-0.59	-0.60	-0.54	-0.52	-0.51
		(-3.08)	(-3.05)	(-2.84)	(-2.85)	(-2.63)

Table VI: Portfolio Analysis of S&P 500 Stocks Sorted by β_{TCCA}

This table reports portfolio sorting tests for estimated S&P 500stock cybercrime beta. The results are based on univariate portfolio sorting based on the β_{TCCA}. First, for each month from December 1998, we form quintile portfolios every month by using NYSE breakpoints, β_{TCCA} is estimated from equation (7), using the last 12 months daily data. Second, we calculate the value-weighted returns for the next month. The first column in the panel reports individual stocks' average cybercrime tracking beta in each relative beta quintile. The remaining columns in each panel present the average excess returns (RET-RF) and risk-adjusted returns (α_3,α_5,α_6, and α_8) for the quintile value-weighted portfolios and the high minus low portfolio in the last row. α_3 is estimated from Fama and French (1993)) three-factor model; α_5 is estimated from Fama and French (2015) five-factor model; α_6 is estimated from Fama and French (2015) five-factor model augmented with the momentum factor; α_8 is estimated from Fama and French (2015) five-factor model augmented with the momentum, short-term and long-term reversal factor. Newey-West adjusted t-statistics are reported in parentheses.

	β_{TCCA}	Excess Return	α_3	α_5	α_6	α_8
Low	-0.63	0.99	0.37	0.32	0.32	0.32
		(3.55)	(2.74)	(2.66)	(2.67)	(2.61)
P_2	-0.18	0.62	0.12	-0.10	-0.11	-0.12
		(2.54)	(1.03)	(-0.98)	(-1.04)	(-1.26)
P_3	0.03	0.61	0.09	-0.02	-0.03	-0.04
		(2.40)	(1.18)	(-0.25)	(-0.29)	(-0.44)
P_4	0.26	0.51	-0.07	-0.20	-0.18	-0.19
		(1.74)	(-0.57)	(-1.73)	(-1.54)	(-1.58)
High	0.78	0.27	-0.45	-0.36	-0.31	-0.29
		(0.70)	(-2.95)	(-2.58)	(-2.34)	(-2.05)
High-Low		-0.72	-0.82	-0.68	-0.63	-0.61
		(-2.64)	(-3.16)	(-2.93)	(-2.80)	(-2.56)

Table VII: Bivariate Portfolio Analysis between Cybercrime Beta and Cybersecurity

This table presents bivariate portfolio sorting results to compare the performance of the two measures, cybercrime tracking beta (β_{TCCA}) and cybersecurity risk, from 10-K filings by Florackis et al. (2023). First, we follow the method proposed by Florackis et al. (2023) in their study to backfill the zeros measures for firms that did not report cyber-related information in 10-K in the early years of the sample. Panel A shows we sort stocks based on cybersecurity risk as a control variable into quintiles. Then, within each cybersecurity portfolio, we sort stocks into quintiles based on β_{TCCA}. Panel B shows that we sort stocks based on our cybercrime tracking beta (β_{TCCA}) as a control variable into quintiles. Then, we sort stocks into quintiles based on cybersecurity within each β_{TCCA} portfolio. The next month's value-weighted portfolio return alphas (α_5 is estimated from Fama and French (2015) five-factor model) are reported in the left sub-panel, and robust t-statistics for 25 portfolios are reported in the right sub-panel. The portfolio sample period is from March 2008 to March 2019 to align the sample periods used in Florackis et al. (2023).

Panel A: Control for Cybersecurity Risk

	α_5					α_t				
β_{TCCA}	1	2	3	4	5	1	2	3	4	5
Low	0.26	0.30	0.32	0.55	0.29	0.75	1.20	1.23	2.23	1.27
P_2	-0.13	0.14	0.32	0.35	0.46	-0.52	0.95	2.31	1.69	2.10
P_3	-0.08	0.27	0.18	-0.24	0.02	-0.51	1.44	1.16	-1.10	0.08
P_4	-0.40	-0.06	0.38	0.22	-0.30	-1.71	-0.30	1.83	1.44	-1.90
High	-0.25	-0.68	-0.71	-0.44	-0.04	-0.68	-2.26	-2.51	-1.61	-0.17
HL	-0.51	-0.98	-1.02	-0.99	-0.32	-0.83	-2.06	-2.03	-3.07	-1.22

Panel B: Control for β_{TCCA}

	α_5					α_t				
Cybersecurity	1	2	3	4	5	1	2	3	4	5
Low	0.26	0.22	-0.21	-0.04	-0.54	0.84	0.77	-0.77	-0.19	-1.25
P_2	0.43	0.02	-0.01	0.01	-0.33	1.47	0.10	-0.05	0.06	-1.07
P_3	0.30	0.21	0.15	0.41	-0.59	1.28	1.34	0.76	1.85	-1.96
P_4	0.26	-0.05	-0.11	0.23	-0.24	1.08	-0.19	-0.54	1.42	-0.78
High	0.23	0.63	-0.11	-0.24	-0.24	0.93	2.78	-0.54	-1.69	-0.93
HL	-0.03	0.41	0.10	-0.20	0.29	-0.10	1.86	0.30	-0.89	0.78