The Anatomy of Cyber Risk*

Rustam Jamilov
London Business School

Hélène Rey
London Business School

Ahmed Tahoun
London Business School

September 2020

PRELIMINARY AND INCOMPLETE.

Abstract

Despite continuous interest from both industry participants and policy makers, empirical research on the economics of cyber security is still lacking. This paper fills the gap by constructing comprehensive text-based measures of firm-level exposure to cyber risk by leveraging machine learning tools developed in Hassan et al. (2019). Our indices capture such textual bigrams as "cyber attack", "ransomware", and "data loss", span 20 years of data, and are available for over 80 counties. We validate our measures by cross-referencing with well-known reported cyber incidents such as the Equifax data breach and the "NotPetya" global ransomware attack. We begin by documenting a steady and significant rise in aggregate cyber risk exposure and uncertainty across the Globe, with a noticeable deterioration in sentiment. The fraction of most-affected firms is gradually shifting from the US towards Europe and the UK. From virtually zero exposure, the financial sector has grown to become one of the most affected sectors in under ten years. We continue by studying asset pricing implications of firm-level cyber risk. First, in windows surrounding conference call announcements, we find direct effects of cyber risk exposure on stock returns. Furthermore, we also find significant within-country-industry-week peer effects on non-affected firms. Second, we document strong factor structure in our firm-level measures of exposure and sentiment and show that shocks to the common factors in cyber risk exposure (CyberE) and sentiment (CyberS) are priced with an opposite sign. Overall, our results suggest that cyber security is a source of *systematic* risk and that firm-level cyber incidents have the potential to grow from idiosyncratic operational disruptions into systemic crises.

*We thank Markus Schwedeler for outstanding research assistance. We thank Richard Portes, Elias Papaioannou for valuable comments and suggestions. Jamilov acknowledges financial support of the Wheeler Institute for Business and Development.

1 Introduction

The World Economic Forum identifies systemic cyber risk as one of the most likely and impactful risks for firms (WEF, 2016). Major institutions have lost nearly $500 billion from operational risk events from 2011 to 2020, predominantly due to cyber attacks (ORX, 2020). The European Systemic Risk Board has recently characterized cyber security as a systemic risk to the European financial system (ESRB, 2020). According to the Center for Strategic and International Studies, cyber-crime caused economic losses up to 1% of global gross output as of 2014 (CSIS, 2014). Recent systemic risk surveys of financial market participants cite cyber security as a Top 2 most challenging risk for managing a firm, falling behind only political risk (BoE, 2018). There is a rapidly escalating interest in cyber monitoring and macroprudential regulation from financial market regulators around the world (Kashyap and Wetherilt, 2019). Cyber attacks pose particularly large threats to trading and banking systems, with new and unforeseen avenues for the propagation of idiosyncratic attacks into systemic crises such as the "cyber bank runs" (Duffie and Younger, 2019).

Despite continuous interest from both industry participants and policy makers, empirical research on the economics of cyber security is grossly lacking. The goal of this paper is to fill this large gap by constructing comprehensive text-based measures of firm-level exposure to cyber risk by leveraging machine learning tools developed in Hassan et al. (2019)[1]. Our method relies on recent advances in computational linguistics and applications of numerical natural language processing (NLP) techqniues to textual information from quarterly firm announcements data provided by Eikon. Conference calls usually take place concurrently with an earnings release and grant a chance for management to describe the overall business position of the company. The vast majority of dialogues of interest, interestingly, take place during the post-announcement Q&A session where investors, industry analysts, and other interested parties can ask questions on various pressing issues.

Our approach is to process all the texts from the announcements and the Q&A sessions and to construct firm-level measures of exposure to cyber risk and uncertainty by identifying and capturing "textual bigrams". These bigrams are ordered combinations of words that relate to some topic of interest. For example, in the Hassan et al. (2019) study authors search for bigrams that are related to political uncertainty. In our case, this flexible approach can identify dialogues related to such topics "cyber attack", "ransomware",

[1]This general approach has been recently applied to the case of epidemic diseases like COVID-19 (Hassan et al., 2020a) and the Brexit vote in the UK (Hassan et al., 2020b)

"data breach", etc. Our complete quarterly dataset is available for 80+ countries and spans the 2002-2020 period.

Our first measure is firm-level total *exposure* to cyber risk. For each transcript, we calculate the number of times each of the following bigrams gets mentioned: "cyber", "cyber security", "cyber risk", "cyber attack", "cyber threat", "spyware", "ransomware", "malware", "phishing", "data breach", "data loss" , "hack", "hacker", and "hacked". Total exposure is then the sum of all of these mentions, normalized by the number of words in each transcript. We compute the aggregate time-series index of cyber risk exposure as a standardized quarterly non-weighted average of the firm-level measure.

Our second and third indices are constructed by following closely the Hassan et al. (2019) methods of measuring firm-level political *uncertainty* and *sentiment*. Specifically, we identify cyber risk related bigrams that are within 20 words of synonyms of "risk" and "sentiment". For the sentiment measure, we are able to filter out positive- and negative-tone words and construct an index of *net sentiment*.

We validate our measurement by manually matching the Eikon firm-level quarterly announcement data with the dataset on realized cyber attacks from the Privacy Rights Clearinghouse. We confirm that our indices of cyber risk exposure and sentiment are strongly correlated with realized attacks. For some of the world's most salient cyber incidents, we extract exact excerpts from the transcripts and highlight the relevant chatter. For example, the 2017 Equifax data breach is associated with a huge spike (fall) in the cyber exposure (sentiment) indices. Another example is the 2017 "NotPetya" global ransomware attack which affected such commercial giants as Maersk and Merck & Co. In our data, we see that in the weeks surrounding the attacks, both of these companies (and many others) carried out prolonged and detailed discussions on the attack, cyber insurance, related legal expenses, etc.

Having constructed our aggregate indices and validated with realized cyber attack data, we now report the main time-series facts on global cyber risk:

Fact 1: *The fraction of conference calls worldwide that discuss cyber risk is growing*. The global intensity of discussions, i.e. number of cyber mentions per call, has also gone up.

Fact 2: *The sentiment surrounding cyber risk is becoming increasingly pessimistic.* The global cyber risk sentiment index has dropped roughly four-fold since 2002.

Fact 3: *Association of cyber-related discussions with uncertainty and risk is growing*. The global cyber risk uncertainty index has risen roughly three-fold since 2002.

Fact 4: *Regional composition of global cyber risk exposure is shifting from U.S. firms to the*

U.K. and Europe. We find sentiment is generally positive in countries like France and more negative in the UK.

Fact 5: *Industrial composition of global cyber risk exposure is shifting towards the financial sector*. The finance industry exhibited virtually 0 exposure back in 2010. However, it's now the second most-affected sector after "Professional Services" (the sector that includes the cyber-sensitive IT consulting firms).

We continue by studying the determinants of most affected firms. We estimate quarterly probit regressions of our measures of cyber risk on an array of balance sheet and income statement characteristics. To that end, we manually merge the Eikon firm announcements data with Compustat. We report three results. First, all three measures are positively correlated with firm-level market capitalization and negatively correlated with firm-level total assets. Second, results are almost completely driven by the finance and services industries. Third, factors such as intangible assets or operational expenses do not appear to have a systematic effect on the likelihood of discussing cyber risk.

Our next major empirical exercise is on the stock market implications of cyber risk. We merge the Eikon dataset with CRSP at the level of a CUSIP. First, we estimate the direct impact of our indices on returns in short windows surrounding quarterly announcements dates. We find that firm-level cyber risk exposure has a negative and significant effects on stock returns. This result is robust to alternative definitions of the event window, controls that include the market factor and firm market cap, and whether returns are value-weighted or unweighted. In these specifications, we impose a stringent combination of either Industry and Country Week fixed effects or Industry Country and Week fixed effects.

Second, we go beyond estimating only direct effects on the affected firms and ask whether *unaffected* firms also experience stock market losses. In other words, are there spillover and network effects of cyber risk discussions within the same week, industry, and country? Formally, our left-hand-side variable is the average stock return of firms that have 0 cyber risk exposure but which are in the same *week, country and industry* with a firm that has had a positive exposure. The right-hand-side variable is positive cyber exposure of affected firms. We find evidence of strong, negative indirect effects: high cyber risk exposure is associated with negative stock returns of firms that have *zero* exposure but are in the same country and industry. Similarly to our direct effects regressions, this result is robust to alternative definitions of the event window, controls that include the market factor and market cap of both affected and unaffected firms, and whether returns are value-weighted or unweighted. We interpret this result as first prima facie evidence

that firm-level cyber risk can be a source of *systematic* risk.

Much of the variation in our aggregate indices of cyber risk exposure, risk, and sentiment is driven by multinational if not worldwide cyber attacks and incidents. Examples include the 2017 "WannaCry" and the 2016-2018 "NotPetya" ransomware attacks. We conjecture that there is *factor structure* in firm-level measures of cyber risk. We construct aggregate pricing factors based on aggregate cyber exposure and sentiment indices - CyberE and CyberS. We construct our factors by extracting residuals from an AR(1) model that is fit onto the raw aggregate indices. Our monthly factors run from 2002:m1 until 2020:m1 and are available for the general public.

We construct 5 CyberE and CyberS one-way sorted stock portfolios, as well as the high minus low portfolio, by regressing firm-level stock returns on the factors and extracting CyberE and CyberS betas. We find that CyberE- and CyberS-sorted portfolios generate annualized spreads in average excess returns of -3.295% and 2.725%, respectively. This shows that stocks which are in the lowest CyberE beta sorted portfolio, i.e. suffer stock market losses when cyber exposure is high, demand equilibrium compensation for holding this additional source of risk. Similarly, stocks that are in the highest CyberS beta sorted portfolio, i.e. suffer stock market losses when cyber sentiment is low, have higher excess returns on average. These return spreads cannot be readily explained away with the CAPM or the 3-factor Fama-French model (Fama and French, 1992) . Similarly, the spread is not correlated with quantile-specific average market values.

In order to estimate the aggregate price of cyber risk, we run the Fama and MacBeth (1973) exercise. We construct 10 CyberE and CyberS sorted stock portfolios from time-series regressions of returns on the two factors. Then, we run cross-sectional regressions of average portfolio excess returns on the CyberE and CyberS betas as well as the three Fama-French factor betas. We find that both CyberE and CyberS are always significant. Moreover, on top of the market factor, CyberE and CyberS can individually explain around 60-80% of the cross-section of stock returns. The mean average pricing error with CyberE (CyberS) and market factors only is 78 (19) basis points per eyar. Overall, we conclude that cyber risk exposure and sentiment are sources of *systematic* risk. In practice, this result maps to the heterogeneous sensitivity towards aggregate, trans-national cyber ransomware attacks and data breaches. Understanding the characteristics of firms that have a higher loading on aggregate cyber risk factors is a matter of first-order priority for future research.

Literature Review

There are several empirical papers that study the impact of cyber risk on economic and financial performance. Kamiya et al. (2020) employ the PRC database and estimate

the effects of realized cyber attacks on firm-level stock returns and subsequent macroeconomic outcomes. Tosun (2019) perform a similar exercise. They also report that short-term market reactions to cyber attacks correlate with increased investors' attention as measured by Google trends. Eisenbach et al. (2020) study how cyber attacks get amplified through the U.S. financial system, with a focus on the wholesale payments network. Haislip et al. (2019) show evidence on indirect effects of realized cyber attacks and find that non-breached peers experience significant negative equity returns around the announcements of breached firms in their industry. Woods et al. (2019) estimate the theoretical distribution of losses due to cyber attacks by leveraging regulatory filings and data on cyber insurance pricing and premia. Biener et al. (2015) study the distinct characteristics of cyber risks compared to other operational risks and emphasize significant problems resulting from interrelated losses, lack of data, and information asymmetries.

All of the aforementioned papers, however, deal with datasets on realized and confirmed cyber incidents. There are considerable issues with regards to this approach. First, there is a well reported problem of considerable underreporting of cyber attacks (Amir et al., 2018). Second, there is potentially a substantial lag (in days, if not weeks) between the day an attack gets reported to authorities and when it actually takes place. This implies that any sort of event study approach with daily asset prices is problematic, particularly if information leaks prior to the disclosure. Our paper makes a methodological contribution to this literature by exploiting detailed quarterly firm announcement data. Under-reporting and time lags are not a problem in our setting because (a) during the Q&A sessions investors and analysts consistently pressure firm executives on issues that the latter could potentially ignore otherwise and (b) earnings announcements get recorded and reported to the general public immediately.

2 Firm-Level Cyber Risk in Firm Announcements Data

2.1 Measurement

We adopt computational linguistics algorithms to the texts of firm-level conference calls from Eikon and tag conversations that in some way relate to cyber risk, data breaches, or hacks. Our general approach follows closely the work of Hassan et al. (2019) on political risk and uncertainty. Our firm-level measure is then constructed by counting the number of exclusive combinations of words that proxy the target synonyms. If an algorithm detects mentioning of cyber risk in any of the bigrams (single words or two-word pairs) in a given transcript, it assigns the value of unity to that particular conference

call. A zero implies that no reference to the particular was made. We run one query on all transcripts in the database per each of the following bigrams: "cyber", "cyber risk", "cyber attack", "cyber threat", "spyware", "ransomware", "phishing", "data breach", "data loss" , "hack", "hacker", and "hacked". Firm-level total exposure to cyber risk aggregated measure of cyber risk is then defined as a simple time-varying total count or dispersion of firm-levels references to any of four cyber sub-topics. The aggregate index of cyber risk exposure is the quarterly unweighted average (standardized) of the firm-level measure. Our approach towards the measures of uncertainty and sentiment are very similar with one exception: we run queries for our cyber risk bigrams conditional on the target words being within a 20-word distance from some synonym for uncertainty and sentiment or attitude. The latter we further bifurcate into positive and negative sentiment.

2.2 Global Cyber Risk Exposure, Uncertainty, and Sentiment

We begin reporting our time-series results with our baseine index of global exposure to cyber risk in Figure 1. We document that the average normalized total count of cyber-related discussions has increased threefold from 2002q1 to 2020q1. This is the intensive margin. Furthermore, the percent of all conference calls with at least one mentioning of cyber-related risks has increased from roughly 0% in 2002 to 2-3% in 2020. This is the extensive margin. Overall, global exposure to cyber risk has increased both in terms of the number of unique affected transcripts per quarter as well as the number of discussions per transcript.

Figure 2 plots our time-series index of global uncertainty from cyber risk. This index has spiked considerably in 2015-2017, potentially tracking the cyber attacks on the Democractic National Convention, the WannaCry ransomware attack, and the NotPetya virus attack. This positive innovation can be interpreted as a persistent negative second moment shock in the spirit of Bloom (2009). In addition to the rise in the frequency of idiosyncratic and aggregate cyber incidents, the market has an increasingly more pessimistic view of the future with regards to cyber security.

Figure 3 plots our time-series index of global sentiment towards cyber risk. We see a clear and persistent negative trend: the index has fallen roughly fourfold since 2002q1 until 2020q1. A priori, it is not obvious that the rise in cyber exposure is in fact a detrimental, negative phenomonon. It is possible that there are just as many winners from elevating cyber risk and uncertainty as there are losers. The winners in this situation could be IT consulting firms, cloud security providers, etc. The fact that the overall sentiment towards cyber risk is increasingly negative suggests to us that the fraction of losers is large

and growing.

2.3 Heterogeneity by Regions, Industries, and Topics

Figure 4b decomposes the global cyber risk exposure index by the country of origin. Each firm in the Eikon data reports its national headquarters. We do not observe the markets that each firm operates in. Panel (a) in the Figure depicts the percent of all transcripts, per year, with cyber riks related discussions, i.e. the extensive margin, and much like our baseline Figure 1 index. Panel (b) shows the regional composition of all cyber risk discussions, in percent. We observe that the vast majority of cyber chatter originats in US firms. However, this trend has been going through a structural change since about 2012. The fraction of calls originating in Europe, the UK, and Africa are steadily increasing. Within the European category, the most affected countries are France and Germany.

Figure 5b decomposes the global exposure index by firm industry, proxied by the two-digit NAICS codes. Again, Panel (a) reports the fraction of all transcripts with non-zero cyber risk related discussions and panel (b) shows the industrial composition of all discussions in percent. We document that the IT and services sectors (which include various IT-related consulting companies) have historically dominated our exposure measures, and understandibly so. However, since about 2012 the percentage of cyber risk discussions attributed to the finance sector has been steadily growing and currently stands at about 20%. In other words, one fifth of all worldwide cyber risk related discussions now occurs in the finance industry. This compositional change has taken place mostly at the expense of the decline in manufacturing.

Figure 6c decomposes the global exposure index by individual topics. Panel (a) reports the raw total number of times earnings call announcements mention "cyber security", "cyber attack", and "cyber threat". Panel (b) - for "data breach", "data loss", and "ransomware". Finally, panel (c) - for "malware", "phishing", and "spyware". We see that the prevalence of these topics is mostly cyclical with the exception of "cyber security" which has dominated the total count from 2007 until about 2017. There is a huge spike in "ransomware" related chatter, driven by the NotPetya global ransomware worm attack. We observe that a somewhat positive persistent trend in the "malware" topic and some pick-up in "data breach" and "phishing" in the late 2010s.

3 Validation with Reported Cyber Attacks

We now validate our firm-level measures of cyber risk. It is important to confirm that our indices are informative about the dangers of actual cyber attacks. We therefore manually merge the Eikon firm-level data with the PRC database on realized cyber incidents. Because there is no common firm identifier, we employ a variant of the fuzzy search algorithm. Specifically, we create a vector of integers for each firm name in the PRC and Eikon data. Then for each firm name in the PRC data, we take the cosine distance with each Eikon firm name and keep the closest match. To create the vector of integers for a firm name, we count all unique letters, adjacent two-letter, and adjacent three-letter combinations. Finally, we compute a measure of semantic distance (normalized to lie in the zero to unity interval) between firm names in the two datasets. We impose a reasonable cutoff for good and bad matches.

We find that out of roughly 6000 non-public, non-governmental, and non-medical firms in the PRC dataset, 600+ unique firm-incident pairs can be matched to the Eikon data. As a final step, having matched Eikon with PRC, we identify some of the most salient realized cyber attacks in recent memory and tag them in both datasets. The goal of this exercises is to check whether our textual algorithms indeed pick up economically meaningful chatter when we know for sure that they should.

Table 1 reports the results. We present 8 major known and reported cyber incidents. For each event, we document the name of the company, the exact date of the conference call, values on cyber risk exposure and sentiment scales, the precise exceprt from the conference call texts, and our own summary of the invent. Overall, we find that these widely known realized cyber attacks are picked up very well by our indices. For example, the 2017 Equifax data breach has an exposure (sentiment) score of 10 (-10), implying large exposure and very negative market sentiment. Another example is the 2014 Target data breach and loss, when over 100 million individuals lost sensitive information including credit card account data. This event corresponds an exposure (sentiment) value of 19 (-19): outliers in the overall distribution. Of course, by far not every spike in our exposure, uncertainty, or sentiment measure must be or is associated with an actual cyber incident. Most of the time, executive and call participants express concerns about *potential* events, which may or may not ever realize.

4 Firm-Level Cyber Risk and Stock Returns

4.1 Direct Effects

In this section we explore asset pricing implications of our measures of cyber risk. We employ an event study approach to tightly defined windows surrounding firm earnings call announcements. We estimate the impact of total firm-level cyber exposure on average stock returns within a one or three day period around the call date. We impose either industry and country $\times$ week or industry $\times$ country and week fixed effects. We also compute both unweighted and value-weighted firm-window-specific returns.

Table 2 reports the results. We find that an increase in cyber exposure has a strong negative effect on realized stock returns. A 1 standard deviation increase in firm-level cyber exposure reduces stock returns by somewhere between 1.6% and 12.7%, depending on the specification. Our favorite specification is column (7) which reports the estimate of 6.9%, significant at the 1% level. The magnitude of our estimates is greater than what is typically reported in the literature, for example in Kamiya et al. (2020) who use realized cyber attack data from PRC. This implies that their estimates are potentially biased downwards, which would be the case if information leaks between the moment the attack takes place and the day it gets reported to authorities.

4.2 Peer Effects

We now move beyond direct effects on affected firms and ask whether there are indirect peer effects in cyber risk exposure. We regress firm-level cyber exposure on stock returns of the non-affected peer firms, which are in the same industry and country. We average returns over the week when the affected firm has its earnings call announcement. Table 3 reports the results. We find strong evidence of peer effects from firm-level cyber risk exposure. A 1-standard-deviation increase in cyber exposure reduces the returns of within-industry-country peers by between 1.5% and 5.2%. Our favorite specification, column 7, reports the 5.2% estimate. These estimates are notably smaller, in absolute value, than our direct effects estimates. This result suggests that "cyber risk shocks" propagate through the network of corporate peers and get dampened as the distance from the origin grows. We consider this result as our first prima facie evidence for the *systemic* nature of cyber risk.

5 Factor Structure in Cyber Risk and the Cross-Section of Stock Returns

In this section we show that there is factor structure in firm-level measures of cyber risk exposure in sentiment. Aggregate cyber risk exposure and sentiment and *factors* that can help price the cross-section of asset prices. We conjecture that firms that covary more strongly with the cyber risk latent factor are more likely to experience higher excess returns, on average. That is, firms that earn less in states of the world where aggregate cyber risk is high (i.e. low cyber risk beta stocks) must demand higher excess returns in equilibrium. The economic cause of this mechanism is that (a) some firms are fundamentally more reliant on business technologies that are more prone to data breaches and malware attacks and (b) some firms are individually less able to insure against idiosyncratic or aggregate cyber attacks with operational risk capital.

5.1 CyberE and CyberS Pricing Factors

We begin by constructing our two pricing factors. We focus on cyber risk exposure and sentiment. First, we compute the monthly time-series of raw aggregate cyber risk exposure and sentiment, as described earlier in the paper. Second, we fit an AR(1) model onto each time-series and extract the residual. This ensures that we capture *shocks* to cyber risk. Finally, we standardize these residuals. Figure 7 plots our two pricing factors - CyberE (exposure) and CyberS (sentiment). We observe that the two are negatively correlated and that CyberS is more volatile.

5.2 Portfolio Sorting

Our first asset pricing test involves running trailing-window 30-month time-series regressions of firm-level excess returns on either CyberE or CyberS. We always include the market factor and a constant. We require at least 30 observations in these regressions. We extract the distribution of firm-level CyberE and CyberS betas and truncate each at the 1% and 99% levels. For each month, we perform a one-way beta sort with value-weighted average excess returns. Five portfolios are formed and held for one month. Table 4 reports the results for both factors.

We see that average portfolio returns are decreasing in CyberE betas and increasing in CyberS betas. Stocks in the first CyberE quintile have negative CyberE betas and thus on average loose value when aggregate cyber exposure is high. In contrast, stocks in

the highest quintile hedge CyberE growth, paying off precisely when high cyber risk states realize. Similar logic applies to the CyberS factor. The long-short portfolio built on CyberE (CyberS) beta sorted stocks pays an average of -3.295% (2.725%) in returns per year. The third and fourth rows in the table report abnormal returns of each portfolio relative to the CAPM and 3-Factor model Fama and French (1993). We see that the spread portfolios have very large annualized alphas: as high as -3.468 for CyberE and 2.472 for CyberS.

We conclude that both cyber exposure and sentiment can generate an excess returns spread, which cannot be readily explained away by the market or FF-3 factors. Established empirical relationships are in line with our priors and theoretical predictions.

5.3 Fama-MacBeth and the Price of Cyber Risk

Our second asset pricing exercise is the Fama and MacBeth (1973) regression. We formally test whether the CyberE and CyberS factors can explain abnormal returns of CyberE and CyberS-beta sorted portfolios. We repeat the time-series step from before and now form 10 single-sorted portfolios. In the second stage, we run a single cross-sectional regression of average excess returns from the 10 test assets on the factors' betas plus a constant. A good model features a sizable R^2, small constants, and small pricing errors (mean average pricing error, or MAPE).

Table 5 reports the results from the cross-sectional estimation step. We first report results for the CAPM where the market excess return is the only factor. We see that in none of the four cases we explore can CAPM price CyberE or CyberS-beta sorted portfolios. R^2 are low and MAPE is very large. When we introduce our factos we see that R^2 increases by 50 to 90 percentage points. Pricing errors fall substantially. For example, the value-weighted CyberS specification exhibits MAPE of just 19.1 basis points per year when just CyberS is used in the estimation. The R^2 of that specification is 0.95. We also highlight that the point estimates of the prices of risk are quantitatively consistent and statistically significant at the 1% level. In the third column of each specification we also add the Fama-French size and book-to-market factors and observe that our factors are still large and significant. The signs of the coefficients are also correct - they are consistent with the portfolio returns spread discussed earlier and our theoretical motivation for the impact of cyber risk on risk premia.

We conclude that there is strong factor structure in firm-level exposures to and sentiment towards cyber risk. CyberS - our sentiment factor - is particularly potent. This is our second evidence in favor of cyber risk being a systemic risk factor. Differential effects of

aggregate cyber risk on firm-level returns and other outcomes is an important and fruitful avenue for future research.

6 Characteristics of Most Affected Firms

TO BE COMPLETED

7 Discussion: Why Economics of Cybersecurity?

Among Most Challenging Risks for Firms

Firms consistently rank cyber threat as second to only political uncertainty in recent surveys of financial market participants. According to the "Systemic Risk Survey" (SRS) of the Bank of England, cyber threat is the second most cited risk to the UK financial system (BoE, 2018). The SRS is conducted by the BoE on a biannual basis to estimate and track market participants' views of risks to the financial systemic stability and resilience. The 2018H2 survey cites cyber uncertainty as the fastest rising form of risk that has reached its new high as of end of 2018. Roughly 55-50% of respondents currently view cyber attacks as one of the most challenging riskts for management of a firm.

Cyber Uncertainty and Realized Attacks

Both realized cyber attacks and cyber uncertainty could have significant spillovers on the economy. There is a deep-rooted conceptual difference between the direct (and second-order) effects of actual realized cyber attacks and the fear of cyber threats. The former could be measured directly through, for example, stock market outcomes as Kamiya et al. (2020) have done. The latter is more subtle. Discussion and fear of future firm-specific or national or multinational cyber tensions could force a firm into real actions (or inactions) even if such threats never actually materialize. In spirit, our paper is thus most closely related to the works on uncertainty shocks by Bloom (2009) or Bloom et al. (2018), and methodologically to Hassan et al. (2019).

In terms of measurement, our approach is superior to the literature that employs realized cyber attack data. First, there could substantial reputational costs for firms to report cyber incidents voluntarily. In our announcements data, firm executives are "forced" by analysts and investors to discuss topics that they would otherwise potentially wish to ignore. The problem of under-reporting of cyber events is well understood in the literature (Amir et al., 2018) Second, there are considerable time lags between when cyber attacks

get reported to the authorites and when they actually take place. This means that running any kind of event study analysis with daily asset price data is highly problematic.

A New Type of Disasters

The growing number of cyber breaches could complement the growing empirical disaster risk literature. An important feature of cyber attacks is targeted malice and presence of a malignant attacker/criminal. This feature is shared with other forms of acts of terror such as physical terrorism and related disasters (Kashyap and Wetherilt, 2019). In this sense, cyber risk could be rationalized as a new type of disaster risk - both aggregate and not. Equilibrium models with disasters are proving to be exceptionally good at rationalizing numerous financial and macroeconomic puzzles and facts[2] An important feature of the empirical disaster risk literature pioneered by Rietz (1988) and Barro (2006) is a relatively low number of international disasters. In addition, going forward technological progress is likely to minimize direct costs of wars, conflicts, famines etc. The direct effect of disasters, as a result, potentially grossly underestimates its expectational impact on risk premia. Following the aforementioned arguments, cyber risk incidents are likely to grow in number exponentially. To the extent that cyber attacks cause direct economic and financial losses, models of disaster risk could leverage databases on reported cyber attacks (both successful or not) in order to re-evaluate the risk premia implications of disaster uncertainty.

Both Idiosyncratic and Aggregate Shocks

Cyber attacks can be viewed as proxies of negative idiosyncratic or aggregate shocks to financial net worth. In February 2016, it was reported that 30+ fraudulent instructions were issued by cyber criminals via the SWIFT network to transfer over $1 billion from the Federal Reserve Bank of New York accounts belonging to the Central Bank of Bangladesh (Gopalakrishnan and Mogato, 2016). Over $50 million were successfully transferred and never recovered, while the rest was either recovered or prevented via inspections and monitoring. The "Bangladesh Bank Robbery" is a peculiar form of a negative shock to bank net worth. Because it involved only a single institutional victim, was essentially unforecastable, and did not trigger mass second-order spillover effects on the Bangladeshi economy, following the economic modelling tradition I view this event as an uninsurable idiosyncratic negative net worth shock.

In May 2017, a worldwide cyberattack took place that targeted hundreds of thousands of computers in 150 countries (Bodkin et al., 2017). Attackers paralyzed computers with

[2] Gabaix (2012) and Gourio (2012) are important contributions to disasters in business cycle research. See Wachter and Tsai (2015) for a review of recent work on disaster risk in financial economics.

the WannaCry ransomware cryptoworm that took private data hostage and demanded a timely ransom for data release. Hundreds of millions of dollars in damages were lost due to this event. Because the attack was international in nature, affected multiple institutions simultaneously, this shock can be categorized as an aggregate negative net worth shock.

In May of 2018, the Federal Bureau of Investigation (FBI) apparently warned the banks of an imminent large-scale operation attempting to empty ATMs of their holdings, a coordinated cyber crime that would cause costly losses for financial institutions (Kirk, 2018). Once penetrated into banks' financial systems, attackers can install malware that removes limits on payment card accounts and modifies internal ATM systems. Cyber criminals proceed with payment card cloning using data from point-of-sale compromises. Stolen data is then encoded into magnetic stripes on the backs of credit cards. Massive international coordinated cashouts can trigger systemic bank runs. Small-scale attacks have already taken place in Japan, South Africa, and Turkey.

Going forward, the frequency of both idiosyncratic and aggregate cyber shocks to net worth is likely to outnumber the more traditional firm-level or global operational risks like factory malfunctions, accounting scandals, disasters, etc.

An Automation-Cyber Risk Dilemma

If we believe in automation as a trend, then the size and persistence of negative cyber shocks is likely to only grow in the future. Autor et al. (2003), Acemoglu and Restrepo (2017), Martinez (2019) among many others study the intricate role that automation will play in the evoluation of aggregate factor shares and labour income in the 21st century. While quantitative results of this growing literature are inconclusive, trend growth of automation and its net impact on the number and nature of distinct labour tasks as well as on producitivity is likely to be very substantial.

On one hand, trend growth in automation could be viewed as a very persistent positive productivity shock. However, on the other hand advances in digital technology create new avenues for malicious attackers, thiefs, and cyber criminals to exploit the digital architecture and disrupt proper functioning of financial transactions. For example, the emergence of cloud technologies enables firms to store and access huge amounts of data that is crucial for their operation. However, cyber attacks on security protocols of firms that manage such cloud technologies (internally or through outsourcing) is a source of systemic risk - all firms that are linked to the same cloud provider could be affected. Quantitatively, the cost of cyber risk should be taken into count in models of automation-driven growth.

Cyber Networks

Digital innovation and emergence of fintech as a form of payment creates a new channel for the escalation and propagation of cyber attacks. On June 20, 2019 Bank of England announced that for the first time financial technology companies would be granted access to bilateral payment systems with the Bank of England on the level playing field with major commercial banks (Giles and Binham, 2019). Technically, new payment providers such as Facebook would be allowed to store funds overnight in interest-bearing accounts at the central bank. This would facilitate the spread and adoption of Libra, Facebook's digital currency, as a novel form of payment. The end goal of this move is to enable BoE to regulate the fintech sector more efficiently.

This, of course, makes fintech firms a target for cyber criminals. Traditionally, commercial banks have been a routine target of cyber attacks. In the Bank of Bangladesh Heist of 2016, criminals stole over $50+ million via fraudulent transfers from the Federal Reserve Bank of New York accounts belonging to BoB (Gopalakrishnan and Mogato, 2016). But commercial banks are also heavily invested in IT security and are, generally, well prepared for such cyber incidents both in terms of security management and regulatory liquidity buffers (Duffie and Younger, 2019). It remains to be seen how fintech companies will withstand future cyber threats, because access to central banking vaults puts a bounty target on their backs.

8 Conclusion

We build novel firm-level indices of cyber risk exposure, uncertainty, and sentiment. Our approach leverages state-of-the-art techniques from computational linguistics and identifies cyber risk related textual bigrams in the texts of quarterly corporate earnings call announcements. We validate our measure by cross-referencing with the databases on realized cyber attacks. Exposure to cyber risk has a large, negative effect on stock returns in windows surrounding earnings call announcements. We find strong evidence of indirect, peer effects of cyber risk exposure - we trace out the impact on firms that did not discuss anything related to cyber risk but were in the same country and industry as the affected firm (peer). Idiosyncratic firm-level cyber risk has a potential of spreading through corporate networks (input-output, production, stock market, etc) and lead to systemic crises.

There is factor structure in firm-level discussions of and references to cyber risk. We construct the two factors - CyberE (exposure) and CyberS (sentiment) - and make them publically available. Common factors in cyber risk exposure and sentiment track real-life major cyber incidents, have low persistence, and are negatively correlated with each

other. Our factors can help price the cross-section of cyber risk beta sorted equity portfolios. We interpret the factor as a time-varying probability of a major cyber disaster event such as a global data breach or a ransomware attack. Firm exposure to the factors is heterogeneous. Firms that are more sensitive to spikes in aggregate cyber risk, proxied either by increases in CyberE or declines in CyberS, require substantial equilibrium returns compensation.

References

ACEMOGLU, D. AND P. RESTREPO (2017): "Robots and Jobs: Evidence from US Labor Markets," *NBER Working Paper*, 23285.

AMIR, E., S. LEVI, AND T. LIVNE (2018): "Do firms underreport information on cyber-attacks? Evidence from capital markets," *Review of Accounting Studies*, 23.

AUTOR, D., F. LEVY, AND R. J. MURNANE (2003): "The Skill Content of Recent Technological Change: An Empirical Exploration," *Quarterly Journal of Economics*, 118(4).

BARRO, R. (2006): "Rare Disasters and Asset Markets in the Twentieth Century," *Quarterly Journal of Economics*, 121(3).

BIENER, C., M. EING, AND J. H. WIRFS (2015): "Insurability of Cyber Risk: An Empirical Analysis," *Working Paper*, 151.

BLOOM, N. (2009): "The Impact of Uncertainty Shocks," *Econometrica*, 77(3), 623–685.

BLOOM, N., M. FLOETOTTO, N. JAIMOVICH, I. SAPORTA-EKSTEN, AND S. J. TERRY (2018): "Really Uncertain Business Cycles," *Econometrica*, 86(3).

BODKIN, H., B. HENDERSON, L. DONNELLY, AND R. MENDICK (2017): "Government under pressure after NHS crippled in global cyber attack as weekend of chaos looms," *The Telegraph*.

BOE (2018): "Bank of England Systemic Risk Survey," .

CSIS (2014): "Net Losses: Estimating the Global Cost of Cybercrime," *Report*.

DUFFIE, D. AND J. YOUNGER (2019): "Cyber Runs," *Hutchins Center Working Paper*, 51.

EISENBACH, T., A. KOVNER, AND M. J. LEE (2020): "Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis," *Federal Reserve Bank of New York Staff report*, 909.

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

FAMA, E. AND K. FRENCH (1992): "The Cross Section of Expected Stock Returns," *Journal of Finance*, 47(2).

——— (1993): "Common risk factors in the returns on stocks and bonds," *Journal of Financial Economics*, 33(1).

FAMA, E. AND J. MACBETH (1973): "Risk, Return, and Equilibrium: Empirical Tests," *Journal of Political Economy*, 81(3).

GABAIX, X. (2012): "Variable Rare Disasters: An Exactly Solved Framework for Ten Puzzles in Macro-Finance," *Quarterly Journal of Economics*, 127(2).

GILES, C. AND C. BINHAM (2019): "BoE to grant tech companies access to overnight accounts," *Financial Times*.

GOPALAKRISHNAN, R. AND M. MOGATO (2016): "Bangladesh Bank official's computer was hacked to carry out $81 million heist," *Reuters*.

GOURIO, F. (2012): "Disaster Risk and Business Cycles," *American Economic Review*, 102(6).

HAISLIP, J., R. PINSKER, K. KOLEV, AND T. STEFFEN (2019): "The economic cost of cybersecurity breaches: A broad-based analysis," *Manuscript*.

HASSAN, T., S. HOLLANDER, L. V. LENT, AND A. TAHOUN (2019): "Firm-Level Political Risk: Measurement and Effects," *Quarterly Journal of Economics*, 134(4).

——— (2020a): "Firm-Level Exposure to Epidemic Diseases: Covid-19, SARS, and H1N1," *Working Paper*.

——— (2020b): "The Global Impact of Brexit Uncertainty," *Working Paper*.

KAMIYA, S., J. KANG, J. KIM, A. MILIDONIS, AND R. STULZ (2020): "Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms," *Journal of Financial Economics*, Forthcoming.

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

KIRK, J. (2018): "FBI Warns Of Pending Large Scale ATM Cashout Strike," *Bankinfosecurity*.

MARTINEZ, J. (2019): "Automation, Growth and Factor Shares," *Working Paper*.

ORX (2020): "2020 Annual Banking and Insurance Operational Loss Reports," .

RIETZ, T. (1988): "The equity risk premium: a solution," *Journal of Monetary Economics*, 22(1).

TOSUN, O. K. (2019): "Cyber Attacks and Stock Market Activity," *Working Paper*.

WACHTER, J. AND J. TSAI (2015): "Disaster Risk and Its Implications for Asset Pricing," *Annual Review of Financial Economics*, 7.

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

WOODS, D., T. MOORE, AND A. SIMPSON (2019): "The County Fair Cyber Loss Distribution: Drawing Inferences from Insurance Prices," *Working Paper*.

APPENDIX

The Anatomy of Cyber Risk

by Rustam Jamilov, Hélène Rey, Ahmed Tahoun

Figures and Tables

Figure 1: **Global Cyber Risk - Total Exposure**

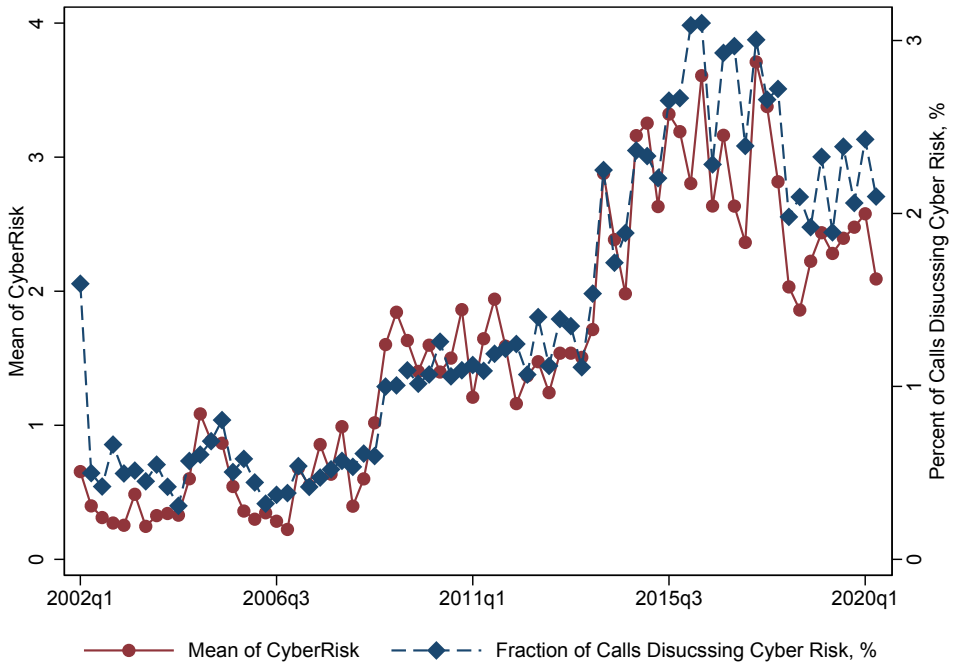


Figure 2: **Global Cyber Risk - Uncertainty**

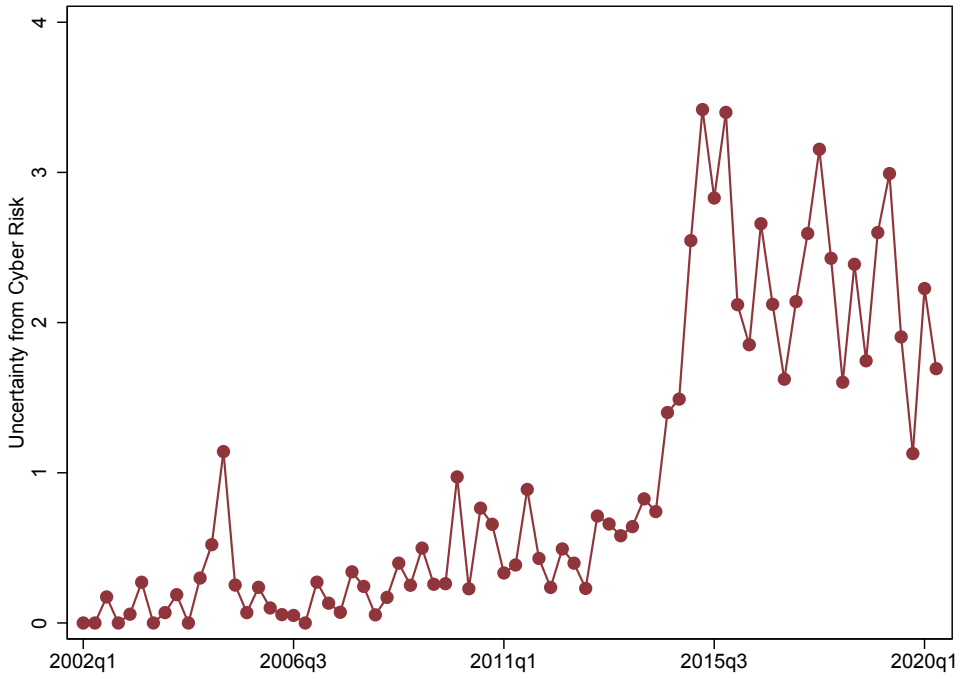


Figure 3: **Global Cyber Risk - Sentiment**

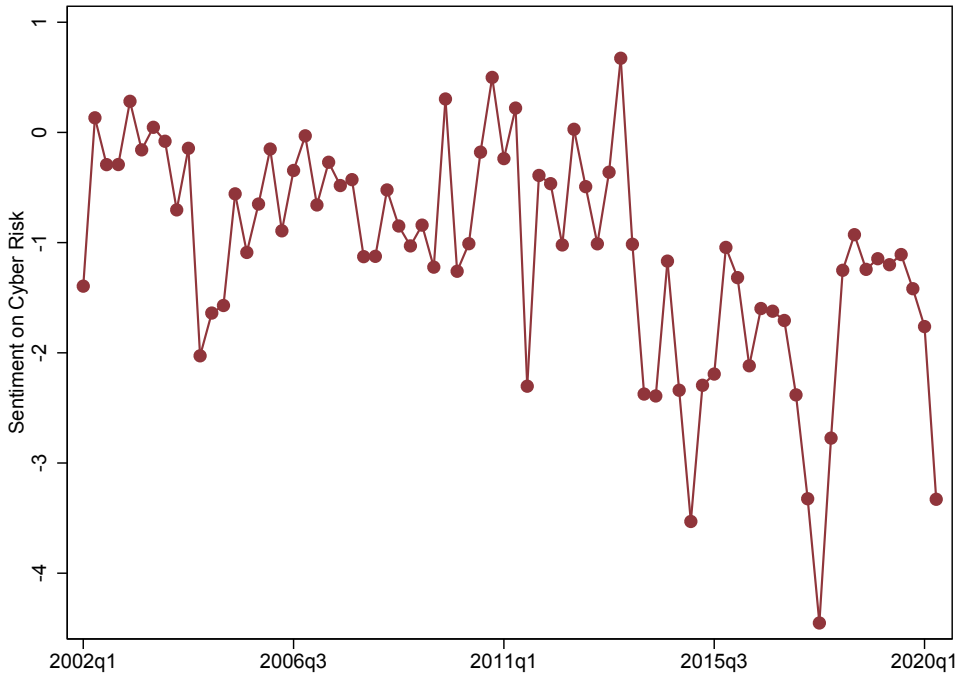
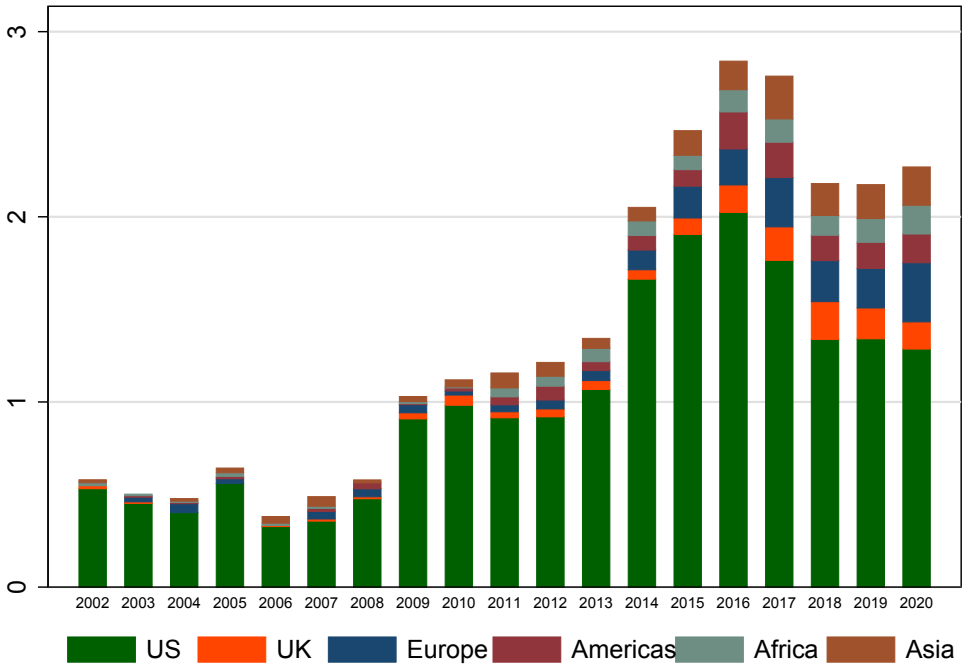
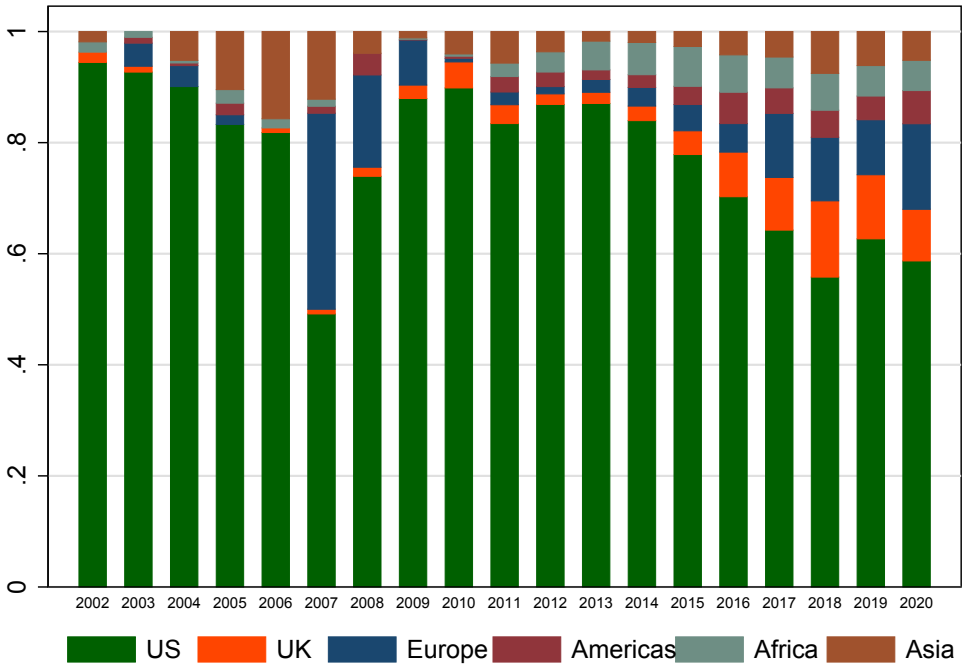


Figure 4: **Global Cyber Risk Exposure - Decomposition by Country**

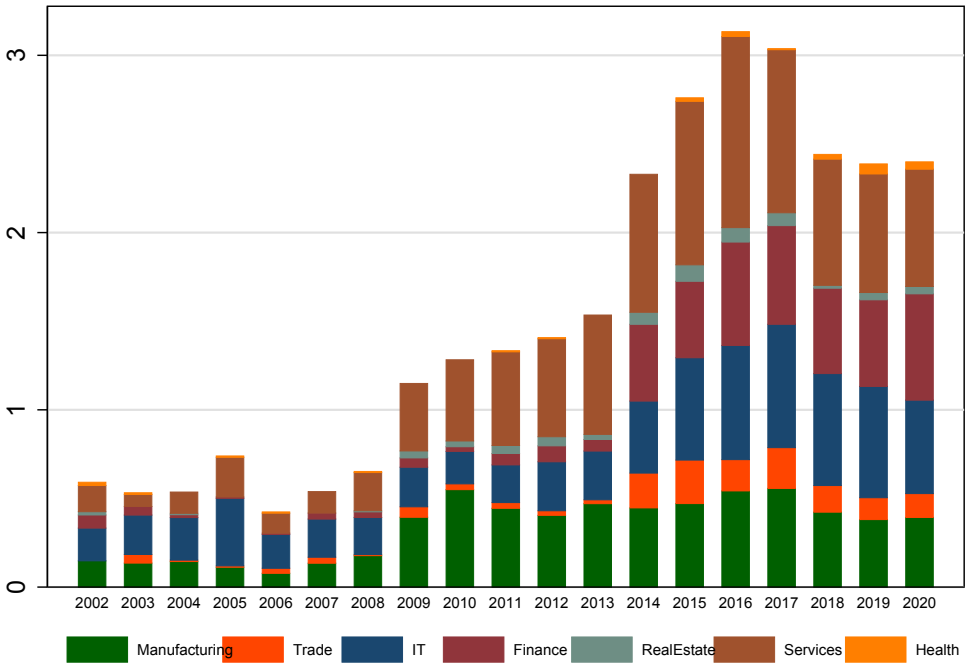


(a) Percent of All Calls Discussing Cyber Risk, by Country

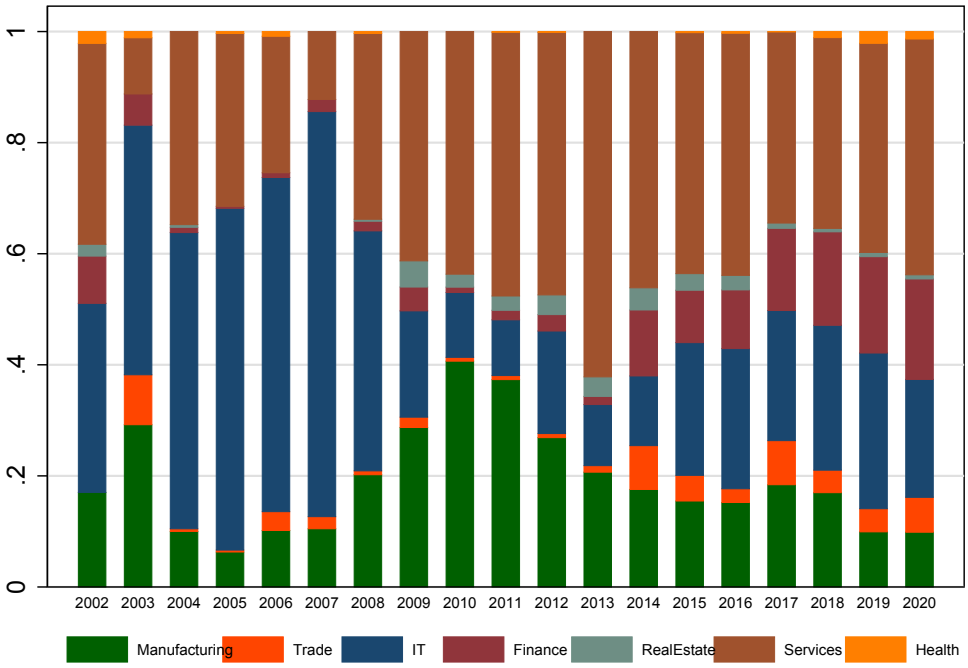


(b) % of Global Cyber Risk Discussions, by Country

Figure 5: **Global Cyber Risk Exposure - Decomposition by Industry**

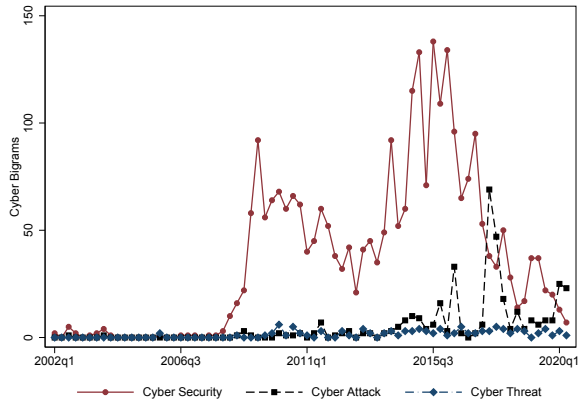


(a) Percent of All Calls Discussing Cyber Risk, by Industry

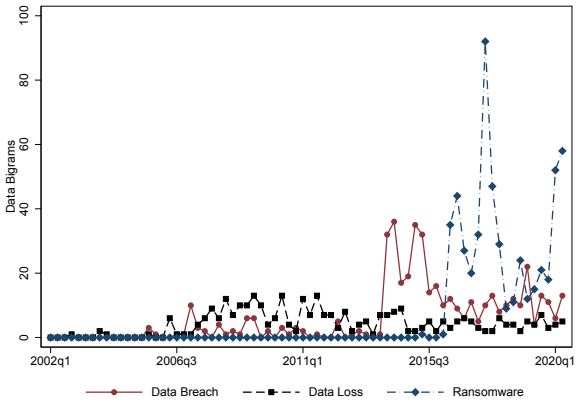


(b) % of Global Cyber Risk Discussions, by Industry

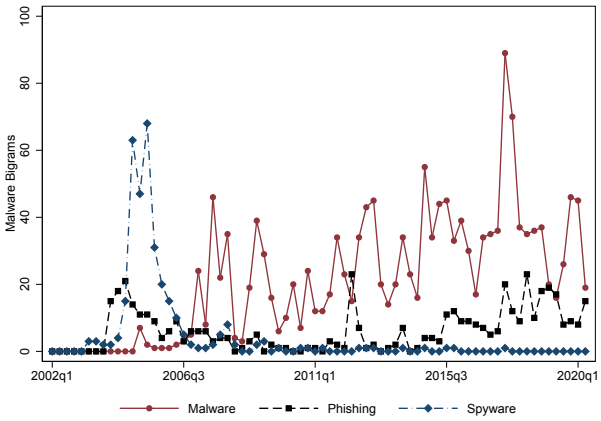
Figure 6: **Global Cyber Risk Exposure - Decomposition by Select Bigrams**



(a) Cyber Security, Cyber Attack, Cyber Threat



(b) Data Breach, Data Loss, Data Ransomware



(c) Malware, Spyware, Phishing

Figure 7: **Cyber Risk Exposure and Sentiment Pricing Factors**

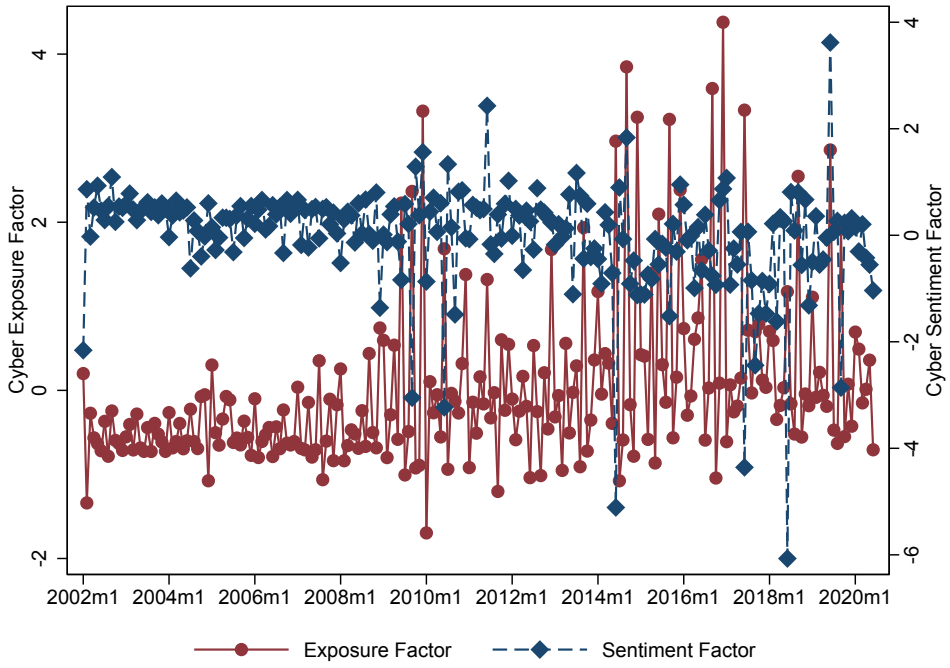


Table 1: **Determinants of Firm-Level Cyber Risk**

	(1) Exposure 1	(2) Exposure 3	(3) Exposure 10	(4) Uncertainty	(5) Sentiment
Market Cap	0.4179***	0.0377	-0.0629***	0.1433***	0.1921***
	(0.0609)	(0.0375)	(0.0173)	(0.0249)	(0.0384)
Total Assets	0.0425	0.2329***	0.1200***	-0.0614**	-0.0581
	(0.0682)	(0.0420)	(0.0194)	(0.0278)	(0.0430)
Leverage	0.2607***	0.0692	-0.0456**	0.0576*	0.1440***
	(0.0813)	(0.0501)	(0.0231)	(0.0332)	(0.0513)
Cash Balances	-0.0561	-0.0776***	-0.0101	-0.0060	-0.0053
	(0.0368)	(0.0226)	(0.0104)	(0.0150)	(0.0232)
Operational Expenses	0.0001***	0.0000	-0.0000	-0.0000	0.0000
	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)
Intangible Assets	0.0000	0.0000	-0.0000	0.0000	0.0000
	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)
Net Income	-0.0001	-0.0001**	-0.0000	-0.0000	0.0001
	(0.0001)	(0.0001)	(0.0000)	(0.0000)	(0.0001)
Country × Industry × Week FE	Yes	Yes	Yes	Yes	Yes
Observations	114858	114858	114858	114858	114858
R^2	0.131	0.093	0.048	0.066	0.089

Notes: Linear probability model estimates. Exposure X takes the value of 1 if cyber exposure index is >=X. Coefficients are scaled by 100 for visibility.

Table 2: **Determinants of Firm-Level Cyber Risk Exposure by Industry**

	(1) Agriculture	(2) Manufacturing	(3) Utilities	(4) Trade	(5) Finance	(6) Services
Market Cap	-0.0623	-0.0040	0.0941	0.1103	1.0351***	1.4763***
	(0.1103)	(0.0691)	(0.1409)	(0.1190)	(0.1319)	(0.2109)
Total Assets	-0.1441	0.0782	0.0271	-0.1432	-0.7139***	-0.8582***
	(0.1210)	(0.0707)	(0.1516)	(0.1427)	(0.1391)	(0.2269)
Leverage	-0.2150	0.0648	-0.0318	0.0462	0.7822***	0.6166**
	(0.1651)	(0.0926)	(0.1945)	(0.1763)	(0.2004)	(0.2814)
Cash Balances	0.1075***	0.2355***	0.0205	0.1586**	-0.0648	0.0825
	(0.0416)	(0.0475)	(0.0686)	(0.0723)	(0.0662)	(0.1530)
Operational Expenses	0.0001	0.0000***	0.0002***	0.0001***	-0.0001**	0.0004*
	(0.0001)	(0.0000)	(0.0001)	(0.0000)	(0.0000)	(0.0002)
Intangible Assets	0.0003***	0.0001***	-0.0000***	-0.0002***	0.0001***	0.0002***
	(0.0001)	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0001)
Net Income	-0.0000	-0.0000	0.0003	0.0007*	-0.0000	-0.0015***
	(0.0002)	(0.0001)	(0.0002)	(0.0004)	(0.0002)	(0.0004)
Country × Week FE	Yes	Yes	Yes	Yes	Yes	Yes
Observations	9113	49043	11432	10670	18737	21656
R^2	0.039	0.018	0.066	0.040	0.053	0.045

Notes: Linear probability model estimates. Exposure X takes the value of 1 if cyber exposure index is >=X. Coefficients are scaled by 100 for visibility.

Table 3: **Determinants of Firm-Level Cyber Risk Uncertainty by Industry**

	(1) Agriculture	(2) Manufacturing	(3) Utilities	(4) Trade	(5) Finance	(6) Services
Market Cap	0.0410	0.0079	0.0588*	0.0000	0.3986***	0.5165***
	(0.0281)	(0.0218)	(0.0301)	(.)	(0.0566)	(0.0958)
Total Assets	-0.0433	-0.0042	-0.0582*	0.0000	-0.2633***	-0.5263***
	(0.0309)	(0.0224)	(0.0324)	(.)	(0.0597)	(0.1030)
Leverage	0.0200	-0.0327	-0.0049	0.0000	0.3120***	0.3903***
	(0.0421)	(0.0293)	(0.0415)	(.)	(0.0860)	(0.1277)
Cash Balance	0.0140	0.0346**	0.0137	0.0000	-0.0438	0.1585**
	(0.0106)	(0.0150)	(0.0147)	(.)	(0.0284)	(0.0694)
Operational Expenses	-0.0000	0.0000	-0.0000	0.0000	0.0000*	-0.0003***
	(0.0000)	(0.0000)	(0.0000)	(.)	(0.0000)	(0.0001)
Intangible Assets	-0.0000	0.0000***	0.0000	0.0000	-0.0000	0.0000
	(0.0000)	(0.0000)	(0.0000)	(.)	(0.0000)	(0.0000)
Net Income	0.0000	-0.0000	0.0001	0.0000	-0.0002*	0.0003
	(0.0000)	(0.0000)	(0.0000)	(.)	(0.0001)	(0.0002)
Country × Week FE	Yes	Yes	Yes	Yes	Yes	Yes
Observations	9113	49043	11432	10670	18737	21656
R^2	0.088	0.007	0.170	.	0.029	0.038

Notes: Linear probability model estimates. Exposure X takes the value of 1 if cyber exposure index is >=X. Coefficients are scaled by 100 for visibility.

Table 4: **Determinants of Firm-Level Cyber Risk Sentiment by Industry**

	(1) Agriculture	(2) Manufacturing	(3) Utilities	(4) Trade	(5) Finance	(6) Services
Market Cap	0.0182	0.0015	-0.0866	0.1048	0.2450***	0.9706***
	(0.0471)	(0.0390)	(0.0730)	(0.0791)	(0.0696)	(0.1421)
Total Assets	-0.0041	-0.0282	0.0331	-0.0274	-0.2130***	-1.0538***
	(0.0517)	(0.0400)	(0.0785)	(0.0948)	(0.0734)	(0.1529)
Leverage	-0.0541	-0.0460	-0.1141	0.1424	0.2057*	0.7693***
	(0.0706)	(0.0523)	(0.1007)	(0.1172)	(0.1058)	(0.1896)
Cash Balance	-0.0188	0.1017***	0.0334	0.0451	-0.0319	0.3390***
	(0.0178)	(0.0269)	(0.0355)	(0.0481)	(0.0350)	(0.1031)
Operational Expenses	0.0000	0.0000	0.0000	-0.0000	-0.0000	-0.0004***
	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0001)
Intangible Assets	-0.0000	0.0000***	-0.0000*	-0.0001***	0.0001***	0.0002***
	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)
Net Income	0.0000	0.0001	0.0002	0.0011***	-0.0001	0.0002
	(0.0001)	(0.0000)	(0.0001)	(0.0003)	(0.0001)	(0.0003)
Country × Week FE	Yes	Yes	Yes	Yes	Yes	
Observations	9113	49043	11432	10670	18737	21656
R^2	0.039	0.009	0.073	0.019	0.047	0.039

Notes: Linear probability model estimates. Exposure X takes the value of 1 if cyber exposure index is >=X. Coefficients are scaled by 100 for visibility.

Table 5: **Firm-Level Cyber Risk and Realized Cyber Attacks**

Company Name	Call Date	Exposure	Sentiment	Exceprt of Discussion	Call summary
Equifax	10.11.2017	10	-10	I have to admit given the impact of –cyber– it is a little more ((difficult)) right now to give ...of the cybersecurity incident These costs were generally for legal –cyber– forensic investigations and other professional services million in accrued expenses ...do we have insurance to cover costs in connection with the –databreach– ((breach)) ((incidents)) with limits in excess of the current amount ...as ((opposed)) to being ...the type of cost that we've incurred	In March 2017, personally identifying data belonging to 147+ million of people was stolen. Incident lead to the company agreeing to a global settlement with the Federal Trade Commission, the Consumer Financial Protection Bureau, and 50 U.S. states and territories. By mos accounts, the largest data breach in U.S. commercial history
State Bank of India	19.05.2017	4	-3	the SBI is doing to check any impact on recent –cyberattack– attack in view of reports about of ATMs in India ...is putting together the technology to prevent any kind of –malware– or cyberhacking to come inside our system to either ((disrupt)) ...((difficult)) to say that we are ready to prevent of –cyber– attacks So if an ((incident)) happens how do we manage ...apart from reporting to the regulators and to the governments –cyber– emergency response team we also share amongst each other to	It was reported that 3.2 million debit cards were compromised in late 2016, affecting major Indian banks including the SBI which was among the worst hit. The breach underwent for several months. SBI announced the blocking and replacement of 500,000+ debit cards

Table 1: **Firm-Level Cyber Risk and Realized Cyber Attacks (Continued)**

Company Name	Call Date	Exposure	Sentiment	Excerpt of Discussion	Call summary
Bank of Montreal	30.05.2018	5	-1	continued (good) performance Now on the topic of the recent –cyber– ((incident)) As Darryl said we are focused on our customers ...for industries like ours Within this changing landscape information and –cybersecurity– security has been an ongoing priority for some time and ...nexus between this accelerated digital transformation and the ((breach)) the –databreach– ((breach)) Ive always thought of this digital transformation as (enhancing) ...is As the technology people will describe it or the –cyber– people describe it as the attack surface increases so is ...we got to be (better) prepared for it Now this –databreach– ((breach)) as far as I can tell and whatever it	Canada's 4th largest financial services institution reported that more than 50,000 accounts across the country were in the hands of hackers. Following the incident disclosure, shares traded down by 0.4%, as per reports.
Capital One	24.10.2019	6	-5	And finally we recognized million of charges associated with the –cyber– ((incident)) that we announced at the end of July These ...to million in certain incremental direct costs associated with the –cyber– ((incident)) response and that we expected to record these costs ...expect to make incremental investments in cybersecurity related to the –cyber– ((incident)) and we expect to absorb the estimated incremental investments ...Sanjay with respect to the public cloud and then the –cyber– ((incident)) while the event occurred in the cloud the ((vulnerability))	An outside individual gained unauthorized access and obtained certain types of personal information about Capital One credit card customers and individuals who had applied for our credit card products. The event affected approximately 100 million individuals in the United States and approximately 6 million in Canada.

Table 1: **Firm-Level Cyber Risk and Realized Cyber Attacks (Continued)**

Company Name	Call Date	Exposure	Sentiment	Excerpt of Discussion	Call summary
Target	26.02.2014	19	-19	performance along with costs related to our recent ((restructuring)) and –databreach– ((breach)) along with small accounting and tax matters As weve . . . of the recent ((slowdown)) in growth weve seen following the –databreach– ((breach)) In Canada in we generated just over billion in . . . headwind and we continue to see the impact of the –databreach– ((breach)) on guest sentiment and traffic We believe that well . . . (beneficial) interest asset and any potential costs related to the –databreach– ((breach)) While this has been a ((challenging)) year we are	Over 100 million individuals were exposed in the attack. Target reported that the information compromised in the attack included mailing addresses, names, email address, phone numbers, and credit and debit card account data.
Maersk	07.11.2017	31	5	third quarter of As youre well aware we had a –cyberattack– attack that impacted the business ((severely)) in July and into August mainly in Maersk Line and Damco This –cyberattack– attack caused volume and revenue ((loss)) as well as additional . . . a quarter with solid global demand growth And adjusting for –cyber– ((loss)) we would have had a flat development in volumes . . . is of course temporary working capital elements related to a –cyberattack– attack We were somewhat ((slower)) on invoicing and therefore our operations were significantly ((hampered)) in the third quarter by the –cyberattack– attack and were certainly not (pleased) with	The NotPetya ransomware attack had a "devastating" effect on Maersk. As per Adam Banks - head of technology and global transport - all end-user devices including 50,000 laptops were destroyed. 1200 applications were destroyed or inaccessible. More than 50% of company servers were destroyed. Any recovered data or devices got immediately re-infected.

Table 1: **Firm-Level Cyber Risk and Realized Cyber Attacks (Continued)**

Company Name	Call Date	Exposure	Sentiment	Excerpt of Discussion	Call summary
Merck	28.07.2017	18	5	on our second quarter results Overall full recovery from the –cyberattack– attack will take some time but we are making steady ...As Ken has outlined the –malware– that infected our computational environment had a very substantial effect ...resources behind our ongoing launches remediation expenses related to the –cyberattack– attack as well as additional RD costs associated with our gears for a moment Let me speak briefly about the –cyberattack– attack on June which as you know affected Merck along	In June 2017, the NotPetya ransomware attack crippled more than 30,000 computers at Merck, as well as 7500 servers (per Bloomberg). Affected screens froze and the following message appeared: "Ooops, your important files are encrypted. ...We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment". The cost was 300 bitcoins or roughly $600,000
Tencent	10.11.2010	17	2	attack by a program which we believe to be a –malware– and its called Kou Kou Bodyguard The malware was created Qihoo which also operates the most (popular) Internet security software Security Guard in China The –malware– (encouraged) users to install it by offering functions such as ...the fact that an Internet security software company actually developed –malware– targeting and affecting an application software We intend to seek ...government authorities However the ensuing ((investigation)) took time while the –malware– spread quickly with s (strong) promotion support In a matter	More than 70 victimes dating back to 2006 were affected, allegedly, by Chinese hacking operations that lasted up until 2011. The series of attacks was orchestrated by Elderwood Group based in Beijing, China. The codeword for the incidends was Operation Aurora. Google was the first company to publically disclose a cyberattack, followed by a series of disclosures across dozens of organizations. (source: Economist.com, Forbes.com, Wired.com)

Table 2: **Cyber Risk and Equity Returns - Direct Effects**

Direct Effects	+- 1 Day				+- 3 Days			
	Unweighted		Weighted		Unweighted		Weighted	
Cyber Exposure	-0.049	-0.038	-0.025	-0.016	-0.070	-0.127	-0.069	-0.121
	(0.012)	(0.015)	(0.008)	(0.012)	(0.007)	(0.053)	(0.009)	(0.049)
Value of Affected	-0.013	-0.030	-0.011	-0.025	0.401	0.245	0.359	0.213
	(0.074)	(0.087)	(0.055)	(0.071)	(0.221)	(0.165)	(0.184)	(0.227)
Value of Non-Affected	0.055	0.0549	0.031	0.031	-0.008	0.011	-0.065	-0.040
	(0.002)	(0.006)	(0.003)	(0.006)	(0.008)	(0.019)	(0.010)	(0.022)
Industry, Country x Week FE	Yes	No	Yes	No	Yes	No	Yes	No
Industry x Country, Week FE	No	Yes	No	Yes	No	Yes	No	Yes
Observations	2180	2382	2180	2382	343	390	343	390
R2	0.364	0.333	0.363	0.335	0.49	0.482	0.48	0.476

Notes: Estimates are in percent, i.e. -0.049 means a decline by 4.9%. Market factors are absorbed by Week FE.

Table 3: **Cyber Risk and Equity Returns - Indirect Effects**

Indirect Effects	+- 1 Day				+- 3 Days			
	Unweighted		Weighted		Unweighted		Weighted	
Cyber Exposure	-0.015	-0.016	-0.020	-0.021	-0.032	-0.027	-0.052	-0.044
	(0.003)	(0.005)	(0.001)	(0.004)	(0.002)	(0.008)	(0.002)	(0.008)
Value of Affected	0.035	0.112	0.070	0.083	0.263	0.202	-0.112	-0.0543
	(0.076)	(0.017)	(0.011)	(0.021)	(0.063)	(0.130)	(0.058)	(0.027)
Value of Non-Affected	-0.022	-0.007	-0.025	-0.021	-0.017	-0.008	-0.094	-0.081
	(0.015)	(0.004)	(0.000)	(0.004)	(0.002)	(0.011)	(0.002)	(0.012)
Industry, Country x Week FE	Yes	No	Yes	No	Yes	No	Yes	No
Industry x Country, Week FE	No	Yes	No	Yes	No	Yes	No	Yes
Observations	2180	2382	2180	2382	343	390	343	390
R2	0.626	0.601	0.608	0.585	0.819	0.787	0.681	0.687

Notes: Estimates are in percent, i.e. -0.015 means a decline by 1.5%. Market factors are absorbed by Week FE.

Table 4: **Cyber Risk Exposure and Sentiment Sorted Portfolios**

Panel A: Cyber-Exposure-Sorted Weighted Portfolios							
	L				H	H-L	t-stat
	(1)	(2)	(3)	(4)	(5)		
Average Excess Returns (%)	9.576	8.399	7.983	6.636	6.281	-3.295	-1.760
Volatility (%)	17.259	14.723	14.812	15.733	17.533	7.559	
Alpha CAPM	-1.848	-0.786	0.995	1.428	1.620	-3.468	-1.700
Alpha FF	-0.0426	0.6864	2.208	2.436	2.952	-2.988	-1.48
Average Market Cap ($bn)	21.310	21.480	21.342	21.151	20.896		
Cyber Exposure beta	-3.145	-1.131	-0.022	1.054	3.010		
Number of Months	189	189	189	189	189	189	
Panel B: Cyber-Sentiment-Sorted Weighted Portfolios							
	L				H	H-L	t-stat
	(1)	(2)	(3)	(4)	(5)		
Average Excess Returns (%)	6.494	7.108	7.649	7.721	9.219	2.725	1.720
Volatility (%)	17.269	14.575	14.711	15.741	17.643	6.649	
Alpha CAPM	0.994	0.235	0.671	0.298	-1.476	2.472	-1.470
Alpha FF	2.340	1.356	1.884	1.728	0.338	2.004	-1.210
Average Market Cap ($bn)	21.106	21.165	21.236	21.368	21.287		
Cyber Sentiment beta	-2.765	-0.918	0.057	1.071	3.039		
Number of Months	190	190	190	190	190	190	

Table 5: **Fama and MacBeth Analysis - Pricing 10 Cyber-Sorted Portfolios**

Panel A: Cyber Exposure Factor		Unweighted			Value Weighted	
Market	-0.06	-0.133	-1.508	-0.0936	-0.137	-1.43
Cyber Exposure		1.144***	1.177**		1.151***	1.161**
HML			-0.607			-0.71
SMB			1.263			1.202
Constant	0.72	0.649**	1.594	0.745	0.663**	1.606
Observations	10	10	10	10	10	10
Rsquared	0	0.578	0.921	0.004	0.599	0.93
MAPE	1.11	0.787	0.317	1.106	0.77	0.289
Panel B: Cyber Sentiment Factor		Unweighted			Value Weighted	
Market	0.3	-0.203***	0.163	0.287	-0.248***	0.106
Cyber Sentiment		-1.086***	-1.098***		-1.137***	-1.137***
HML			0.403			0.313
SMB			0.0984			0.111
Constant	0.33	0.626***	0.276	0.34	0.670***	0.339
Observations	10	10	10	10	10	10
Rsquared	0.09	0.955	0.963	0.079	0.95	0.955
MAPE	0.67	0.175	0.161	0.674	0.191	0.183