The Anatomy of Cyber Risk

Rustam Jamilov
All Souls College, Oxford

Hélène Rey
London Business School,
CEPR, and NBER

Ahmed Tahoun
London Business School

Motivation

Merkel blames Russia for 'outrageous' cyberattack on German parliament

German chancellor says that 2015 hacking attack negatively affects relations with Moscow.

WannaCry cyber-attack cost the NHS £92m after 19,000 appointments were cancelled

Chinese military hackers charged with Equifax cyber attack that hit 15m Britons

Members of People's Liberation Army's hacking unit face US charges over 2017 hack

US Treasury department officials subject to hacking campaign

Department confirms breach as attorney-general says Russia likely culprit behind attack

General election 2019: Labour Party hit by second cyber-attack

12 November 2019

More than one in four UK cyber attacks related to Covid-19

National centre's findings come days after US warned of threat to hospitals from hackers

Vaccines for sale on dark web as criminals target pandemic profits

Cyber attacks on vaccine infrastructure have been widely documented, with theft and fraud expected to rise

Pfizer/BioNTech say EMA breach exposed vaccine documents

Companies say records related to regulatory submission 'unlawfully accessed' on EU regulator's server

This Paper

- **Research question:** Economic implications of growing cyber risk concerns.
- **Data:** Quarterly earnings conference calls of listed firms.
- **Measurement:** Natural language processing and textual analysis.
- **Contribution:** A new quarterly firm-level dataset.

This Paper

- **Research question:** Economic implications of growing cyber risk concerns.
- **Data:** Quarterly earnings conference calls of listed firms.
- **Measurement:** Natural language processing and textual analysis.
- **Contribution:** A new quarterly firm-level dataset.

- **Main findings:**
  - Cyber risk is priced in the equity option market.
  - Spillover effects. Systemic risk.
  - Global cost of cyber risk is $200+ billion per year.
  - International distribution of cyber - gravity model with portfolio holdings.

Literature

- **Cyber risk**: Biener et al. (2015), Makridis and Dean (2018), Kashyap and Wetherilt (2019), Duffie and Younger (2019), Woods et al. (2019), Aldasoro et al. (2020), Crosignani et al. (2020), Kamiya et al. (2021), Eisenbach et al. (2021), Akey et al. (2021), Tosun (2021), Anhert et al. (2022), Adeney et al. (2022), Engels et al. (2022)
- **Cyber risk + text**: Jiang et al. (2020), Lhuissier and Trippier (2021), Florackis et al. (2022)
- **Earnings announcements:** Patell and Wolfson (1979), Hollander et al. (2010), Huang et al. (2018), Hassan et al. (2019), Hassan et al. (2020), Hassan et al. (2022a, 2022b), Sautner et al. (2022)
- **Text:** Loughran and McDonalnd (2011), Baker et al. (2016), Koijen et al. (2016), Loughran and McDonald (201), Gentzkow et al. (2019), Neuhierl and Weber (2020), Engle et al. (2020)
- **Option markets:** Hentschel (2003), Beber and Bradt (2006), Vanden (2008), Bollersev et al. (2009), Carr and Wu (2009), Chang et al. (2013), Bali and Zhou (2016), Kelly et al. (2016), Ilhan et al. (2020)

Data

- **Earnings calls:** Thomson Reuters' StreetEvents
  - 348,393 English-language transcripts of firms listed in the U.S.
  - Typically 1 transcript per quarter, 45 minute duration, ca. 8,000 words
  - Structure: speech by management, Q&A session with financial analysts
  - Common firm identifier (Global Company Key, GVKEY)

Data

- **Earnings calls:** Thomson Reuters' StreetEvents
  - 348,393 English-language transcripts of firms listed in the U.S.
  - Typically 1 transcript per quarter, 45 minute duration, ca. 8,000 words
  - Structure: speech by management, Q&A session with financial analysts
  - Common firm identifier (Global Company Key, GVKEY)
- **Advantages:**
  - Cyberattacks are under-reported; our focus on *exposure* is less prone to selection issues
  - Earnings calls are forward-looking and have active Q&A sessions
  - Can capture "soft" signals and analyst attention

Data

- **Stock options:** OptionMetrics' Ivy DB Volatility Surface
  - Implied volatility (price risk): $IV_{j,t,m}$, $m > t$
  - Variance risk premium (variance risk): $VRP_{j,t,m} = IV^2_{j,t,m} - RV^2_{j,t,m}$
  - Implied volatility slope (downside risk): $IV_{j,t} = \beta_0 + \boxed{SlopeD_j} Delta_{j,t} + \varepsilon_{j,t}, \forall j$

Data

- **Stock options:** OptionMetrics' Ivy DB Volatility Surface
  - Implied volatility (price risk): $IV_{j,t,m}$, $m > t$
  - Variance risk premium (variance risk): $VRP_{j,t,m} = IV^2_{j,t,m} - RV^2_{j,t,m}$
  - Implied volatility slope (downside risk): $IV_{j,t} = \beta_0 + \boxed{SlopeD_j} Delta_{j,t} + \varepsilon_{j,t}, \forall j$
- **Realized cyberattacks:** Privacy Rights Clearinghouse
  - Manually merge with earnings calls data

Data

- **Stock options:** OptionMetrics' Ivy DB Volatility Surface
  - Implied volatility (price risk): $IV_{j,t,m}$, $m > t$
  - Variance risk premium (variance risk): $VRP_{j,t,m} = IV^2_{j,t,m} - RV^2_{j,t,m}$
  - Implied volatility slope (downside risk): $IV_{j,t} = \beta_0 + \boxed{SlopeD_j} Delta_{j,t} + \varepsilon_{j,t}, \forall j$
- **Realized cyberattacks:** Privacy Rights Clearinghouse
  - Manually merge with earnings calls data
- **Stock prices:** CRSP
- **Firm data:** Compustat

Example Earnings Call Snippet: Equifax 2017

Quarter	Company	CyberRisk$^{A}_{i,t}$	Text Snippet
2017q4	Equifax Inc.	38	has there been any further progress in identifying whether **the hack was done by a foreign -state- actor** now bloomberg had run a story saying that there was evidence of that but it didnt sound like anything definitive has come out when is there a pronouncement about that yes what we have as i have my -testimony- declared theres no we; **whats your overall level of comfort that the majority of the cyber costs would be -cyberevent- by -insurance- as opposed to being more equifax ultimately yes so we were not going to specifically disclose the specific amount of the coverage** and in general we believe that the type of -cost- that weve incurred related to the cyber event are indeed under the general structure of the -policy- and were currently in discussions with the insurers around completing around moving forward with -insurance- claims and we would expect to make very good progress in this quarter on that process understood a quick final question from me you mentioned; help frame how youre thinking about **total costs of the -breach- and how much youre accruing for -breach- costs** beyond the; have insurance to cover costs in connection with the data -breach- -incidents- with limits in excess of the current amount of; **much of the usis -decline- was due to the data -breach- compared to mortgage market** -decline- and if you anticipate customer; time its certainly -lost- its only been months since the -cyberevent- event so the discussions are ongoing so we were characterizing;

- The 2017 Equifax data breach, one of the worst in known history.
- Many dimensions: insurance, legal. Q&A session important.

Cyber Risk Terms Dictionary

- Start with a broad pre-defined dictionary of keywords related to cyber

Cyber Risk Terms Dictionary

- Start with a broad pre-defined dictionary of keywords related to cyber
- **Sources:** Financial Stability Board, National Cyber Security Centre, Cybersecurity and Infrastructure Security Agency
  - Credible institutions
  - Information aggregators on all issues cyber-related
  - Vocabularies are available online

Cyber Risk Terms Dictionary

- Start with a broad pre-defined dictionary of keywords related to cyber
- **Sources:** Financial Stability Board, National Cyber Security Centre, Cybersecurity and Infrastructure Security Agency
  - Credible institutions
  - Information aggregators on all issues cyber-related
  - Vocabularies are available online
- **In total:** 275 scraped terms

Cyber Risk Terms Dictionary

- Start with a broad pre-defined dictionary of keywords related to cyber
- **Sources:** Financial Stability Board, National Cyber Security Centre, Cybersecurity and Infrastructure Security Agency
  - Credible institutions
  - Information aggregators on all issues cyber-related
  - Vocabularies are available online
- **In total:** 275 scraped terms
- **Examples:** “data”, “cyber alert”, “malware”, “bug”, “breach”, “vulnerability assessment”, “pharming”, “botnet”, “patch management”, etc.

Dictionary Validation

- **Concern**: are we picking up other risks?

Dictionary Validation

- **Concern**: are we picking up other risks?
- **Validation**: use realized cyberattacks.

Dictionary Validation

- **Concern**: are we picking up other risks?
- **Validation**: use realized cyberattacks.
  1. Given $\mathbb{C}$ the set of all terms in starting dictionary, build: $\text{TermInd}_{i,t}^{c} = 1[c \in \mathbb{B}_{i,t}], \quad \forall c \in \mathbb{C}$
  2. Run logistic regression of $\text{TermInd}_{i,t}^{c}$ on cyberattack indicator that equals 1 if the firm *i* gets cyberattacked within the next k quarters
  3. Control for time and industry fixed effects + size, beta, age, Tobin's Q, leverage, liquidity, intangibles / assets, and operational costs / assets
  4. Keep only terms with a positive effect on future attack likelihood

Dictionary Validation

- **Concern**: are we picking up other risks?
- **Validation**: use realized cyberattacks.
  1. Given $\mathbb{C}$ the set of all terms in starting dictionary, build: $\text{TermInd}_{i,t}^{c} = 1[c \in \mathbb{B}_{i,t}], \quad \forall c \in \mathbb{C}$
  2. Run logistic regression of $\text{TermInd}_{i,t}^{c}$ on cyberattack indicator that equals 1 if the firm *i* gets cyberattacked within the next k quarters
  3. Control for time and industry fixed effects + size, beta, age, Tobin's Q, leverage, liquidity, intangibles / assets, and operational costs / assets
  4. Keep only terms with a positive effect on future attack likelihood
- Final set $\tilde{\mathbb{C}}$ includes 117 unique terms

Dictionary Validation

- **Concern**: are we picking up other risks?
- **Validation**: use realized cyberattacks.
  1. Given $\mathbb{C}$ the set of all terms in starting dictionary, build: $\text{TermInd}_{i,t}^{c} = 1[c \in \mathbb{B}_{i,t}], \quad \forall c \in \mathbb{C}$
  2. Run logistic regression of $\text{TermInd}_{i,t}^{c}$ on cyberattack indicator that equals 1 if the firm *i* gets cyberattacked within the next k quarters
  3. Control for time and industry fixed effects + size, beta, age, Tobin's Q, leverage, liquidity, intangibles / assets, and operational costs / assets
  4. Keep only terms with a positive effect on future attack likelihood
- Final set $\tilde{\mathbb{C}}$ includes 117 unique terms
- **20 most frequent terms**: "data", "software", "digital", "network", "accountability", "availability", "computer", "compromise", "disclosure", "spam", "router", "vulnerabilitymanagement", "domain", "encryption", "firewall", "antivirus", "confidentiality", "datasecurity", "bug", "app".

Firm-Level Cyber Risk Exposure

- Construct baseline quarterly measures of firm-level cyber risk exposure

$$\text{CyberRisk}^{A}_{i,t} = \sum_{b}^{B_{i,t}} \left(1[b \in \tilde{\mathbb{C}}]\right)$$

$$\text{CyberRisk}^{R}_{i,t} = \frac{\sum_{b}^{B_{i,t}} \left(1[b \in \tilde{\mathbb{C}}]\right)}{B_{i,t}}$$

$$\text{CyberRisk}^{I}_{i,t} = 1\left[\text{CyberRisk}^{A}_{i,t} > 0\right]$$

Firm-Level Cyber Risk Exposure

- Construct baseline quarterly measures of firm-level cyber risk exposure

$$\text{CyberRisk}^{A}_{i,t} = \sum_{b}^{B_{i,t}} \left(1[b \in \tilde{\mathbb{C}}]\right)$$

$$\text{CyberRisk}^{R}_{i,t} = \frac{\sum_{b}^{B_{i,t}} \left(1[b \in \tilde{\mathbb{C}}]\right)}{B_{i,t}}$$

$$\text{CyberRisk}^{I}_{i,t} = 1\left[\text{CyberRisk}^{A}_{i,t} > 0\right]$$

- Canonical weighted scheme representation: $1[b \in \mathbb{C}] \times w_b$
  - $1[b \in \mathbb{C}]$ is term frequency
  - w_b is binary term weight based on cyberattack logistic regressions

Topical Analysis

- Topics: insurance, law, social media, cryptocurrencies, politics, sentiment, uncertainty, epidemic diseases

Topical Analysis

- Topics: insurance, law, social media, cryptocurrencies, politics, sentiment, uncertainty, epidemic diseases
- **Novel** dictionaries for the insurance, law, social media, and cryptocurrency topics

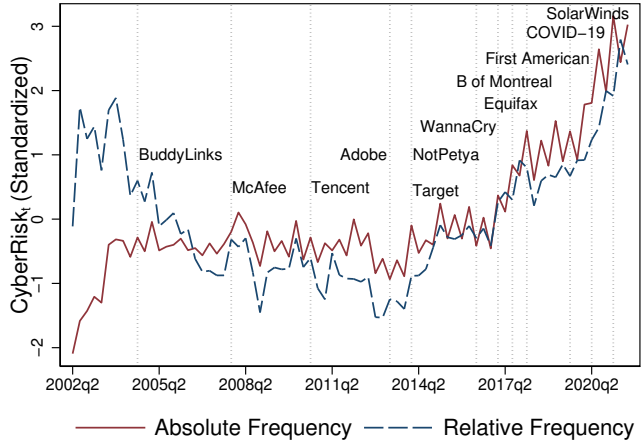
Topical Analysis

- Topics: insurance, law, social media, cryptocurrencies, politics, sentiment, uncertainty, epidemic diseases
- **Novel** dictionaries for the insurance, law, social media, and cryptocurrency topics
- Topical dictionary validation
  1. Identify cyber terms that are in close proximity to a topical term: $\text{TopicInd}_{i,t}^{c,k} = 1[c \in \mathbb{B}_{i,t}] \times 1[c - k] < Z, \quad \forall c \in \mathbb{C}$
  2. Run the same dictionary validation test with realized cyberattacks

Topical Analysis

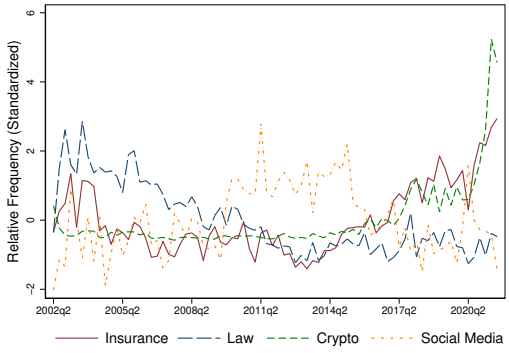
- Topics: insurance, law, social media, cryptocurrencies, politics, sentiment, uncertainty, epidemic diseases
- **Novel** dictionaries for the insurance, law, social media, and cryptocurrency topics
- Topical dictionary validation
  1. Identify cyber terms that are in close proximity to a topical term: $\text{TopicInd}_{i,t}^{c,k} = 1[c \in \mathbb{B}_{i,t}] \times 1[c - k] < Z, \quad \forall c \in \mathbb{C}$
  2. Run the same dictionary validation test with realized cyberattacks
- Construct 9 topical measures as: $\text{CyberRisk Topic}_{i,t}^{R} = \frac{\sum_{b}^{B_{i,t}} \left(1[b \in \tilde{\mathbb{C}}^{\text{Topic}}]\right)}{B_{i,t}}$

Cyber Risk Exposure over Time

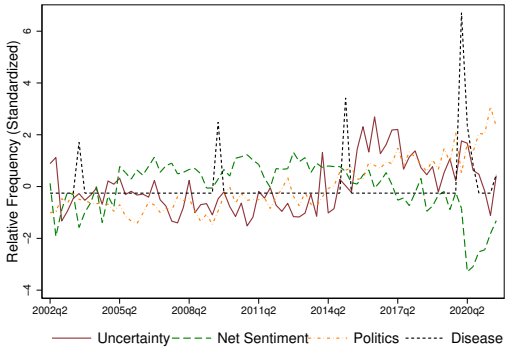


- Global cyber risk exposure has risen 3-fold over 2015-2022
- Peak reached during the COVID-19 pandemic

Cyber Risk by Topic over Time



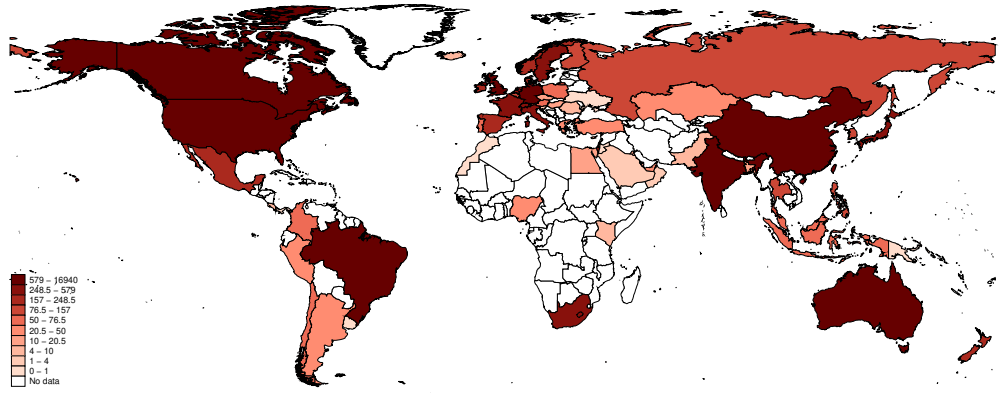
(A) Novel Topics



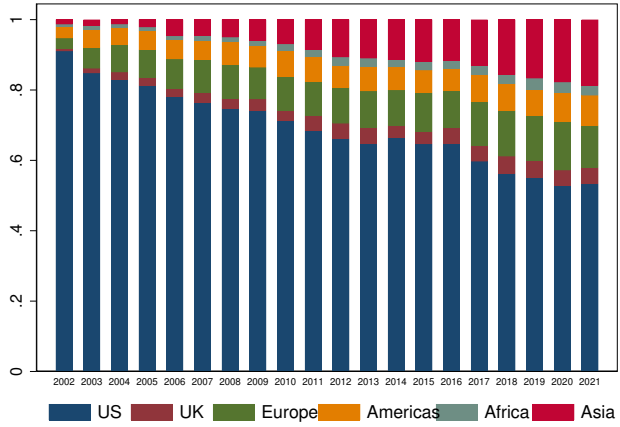
(B) Topics from Hassan et al. (2019)

- Insurance topical index has the highest correlation with CyberRisk_t
- Net Sentiment is negative on average and negatively correlated with CyberRisk_t

CyberRisk$^{A}_{it}$ Regional Decomposition in 2021

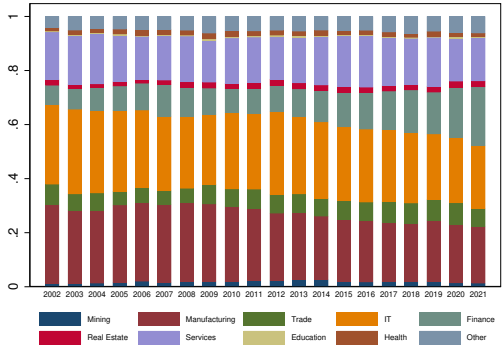


$\text{CyberRisk}^{A}_{it}$ Regional Decomposition over Time

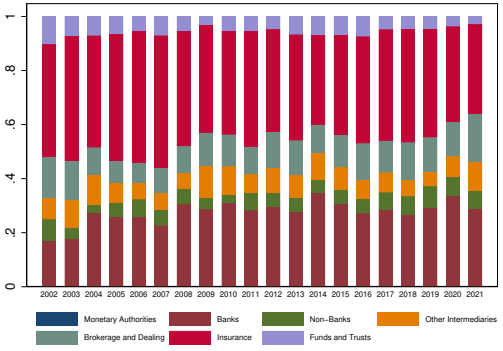


- Structural shift away from the U.S.
- Cyber risk is an increasingly global source of risk

CyberRisk$^{A}_{it}$ Industrial Decomposition over Time



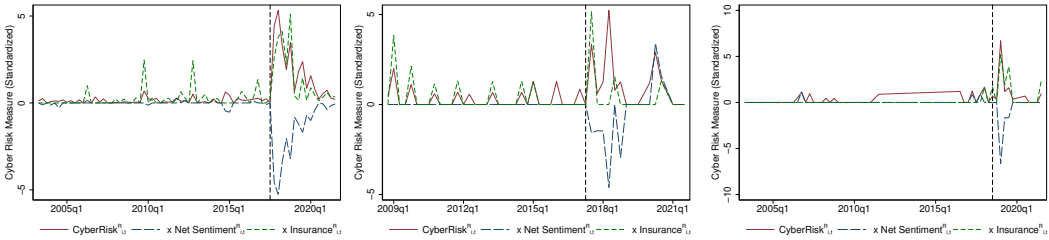
(A) All Industries



(B) Finance Sub-Sectors

- Most affected industries in 2021: IT, manufacturing, finance, services, trade
- Finance sub-sectors: 45% banks, 30% insurance, 20% broker-dealers, 5% funds

Select Case Studies of Cyberattacked Firms



(A) Equifax (B) Bank of Montreal (C) Marriott

1. Equifax: 2017 data breach. One of the biggest data compromises in history
2. Bank of Montreal: 2017-2018 online banking breach. 100K+ affected customers in two separate attacks
3. Marriott Hotels: 2018 breach affecting 300+ million customers. Fined £18 mln in U.K. by privacy watchdog

Further Validation Tests

1. Manual reading of 200+ transcripts of exposed and unaffected firms ✓

Further Validation Tests

1. Manual reading of 200+ transcripts of exposed and unaffected firms ✓
2. More snippets Go
   - Earnings calls around known reported cyberattacks
   - Large cybersecurity firms

Further Validation Tests

1. Manual reading of 200+ transcripts of exposed and unaffected firms ✓
2. More snippets Go
   - Earnings calls around known reported cyberattacks
   - Large cybersecurity firms
3. More case studies Go

Further Validation Tests

1. Manual reading of 200+ transcripts of exposed and unaffected firms ✓
2. More snippets Go
   - Earnings calls around known reported cyberattacks
   - Large cybersecurity firms
3. More case studies Go
4. Predicting cyberattacks Go
   - Our measures predict attacks 8, 4, and 1 quarter into the future

Further Validation Tests

1. Manual reading of 200+ transcripts of exposed and unaffected firms ✓
2. More snippets Go
   - Earnings calls around known reported cyberattacks
   - Large cybersecurity firms
3. More case studies Go
4. Predicting cyberattacks Go
   - Our measures predict attacks 8, 4, and 1 quarter into the future
5. Comparison with Florackis et al. (2022) Go
   - FLMW use annual 10-K filings of listed firms and textual analysis to build measures of cybersecurity risk
   - Our indices and index-based stock factors are (not perfectly) correlated

Firm-Level Implications of Cyber Risk Exposure

- Does cyber risk *exposure* have economic implications?

Firm-Level Implications of Cyber Risk Exposure

- Does cyber risk *exposure* have economic implications?
- High CyberRisk_{it} can indicate **uncertainty** about
  - Operational capabilities, resilience of computer and network systems
  - Likelihood of future incidents, which may or may not realize
  - And thus potential direct monetary or indirect reputational losses

Firm-Level Implications of Cyber Risk Exposure

- Does cyber risk *exposure* have economic implications?
- High CyberRisk_{it} can indicate **uncertainty** about
  - Operational capabilities, resilience of computer and network systems
  - Likelihood of future incidents, which may or may not realize
  - And thus potential direct monetary or indirect reputational losses
- Cross-sectional **implication**: costs of protection against risks should price this in

Firm-Level Implications of Cyber Risk Exposure

- Does cyber risk *exposure* have economic implications?
- High CyberRisk_{it} can indicate **uncertainty** about
  - Operational capabilities, resilience of computer and network systems
  - Likelihood of future incidents, which may or may not realize
  - And thus potential direct monetary or indirect reputational losses
- Cross-sectional **implication**: costs of protection against risks should price this in
- Operationalize with **option market measures** of price, variance, and downside risk

Firm-Level Implications of Cyber Risk Exposure

- Does cyber risk *exposure* have economic implications?
- High CyberRisk_{it} can indicate **uncertainty** about
  - Operational capabilities, resilience of computer and network systems
  - Likelihood of future incidents, which may or may not realize
  - And thus potential direct monetary or indirect reputational losses
- Cross-sectional **implication**: costs of protection against risks should price this in
- Operationalize with **option market measures** of price, variance, and downside risk
- We also look at stock market and balance sheet outcomes

Firm-Level Option Market Effects

Independent Variable:	$\text{CyberRisk}^{I}_{i,t}$			$\text{CyberRisk}^{A}_{i,t}$			$\text{CyberRisk}^{R}_{i,t}$ (std.)		
Dependent Variable (std.):	IV	VRP	SlopeD	IV	VRP	SlopeD	IV	VRP	SlopeD
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Cyber Risk	0.030***	0.015**	0.016***	0.006***	0.002**	0.003***	0.022***	0.011***	0.006**
	(0.005)	(0.006)	(0.004)	(0.001)	(0.001)	(0.001)	(0.003)	(0.003)	(0.003)
Controls	✓	✓	✓	✓	✓	✓	✓	✓	✓
Firm FE	✓	✓	✓	✓	✓	✓	✓	✓	✓
Time FE	✓	✓	✓	✓	✓	✓	✓	✓	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	105,272	105,263	105,192	105,272	105,263	105,192	102,749	102,740	102,662
R^2	0.793	0.380	0.855	0.793	0.380	0.855	0.791	0.379	0.855

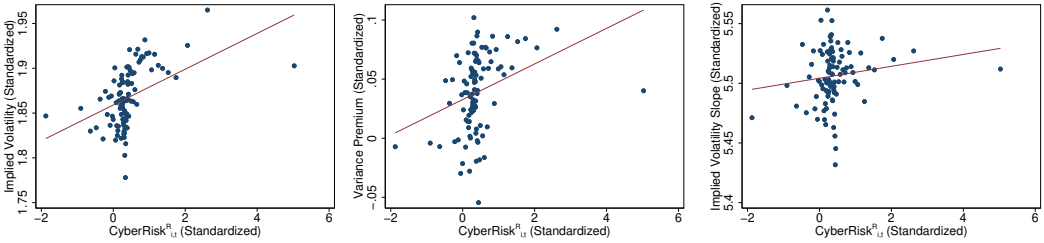
- Cyber risk is priced in the equity option market.

Firm-Level Economic Effects

Independent Variable:	$\text{CyberRisk}^{I}_{i,t}$			$\text{CyberRisk}^{A}_{i,t}$		
Dependent Variable (std.):	$\text{RoA}_{i,t+1}$	$\text{CashFlow}_{i,t+1}$	$\text{Valuation}_{i,t}$	$\text{RoA}_{i,t+1}$	$\text{CashFlow}_{i,t+1}$	$\text{Valuation}_{i,t}$
	(1)	(2)	(3)	(4)	(5)	(6)
Cyber Risk Measure	-0.027***	-0.024***	-0.006***	-0.007***	-0.006***	-0.001**
	(0.006)	(0.006)	(0.002)	(0.001)	(0.001)	(0.000)
Controls	✓	✓	✓	✓	✓	✓
Firm FE	✓	✓	✓	✓	✓	✓
Time FE	✓	✓	✓	✓	✓	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	99060	99060	86188	99060	99060	86188
R^2	0.410	0.455	0.965	0.410	0.455	0.965

- Cyber risk impacts economic performance.

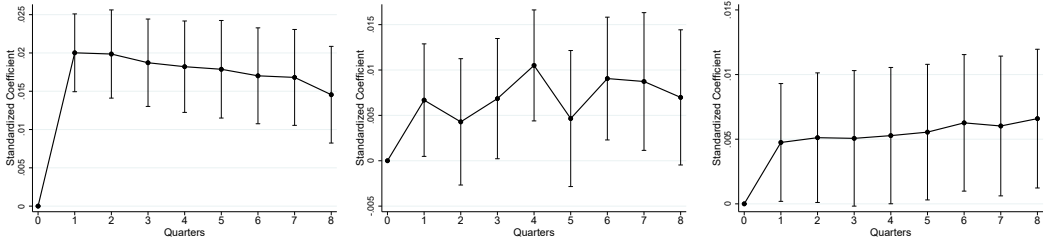
Firm-Level Option Market Effects



(A) Implied Volatility (B) Variance Risk Premium (C) Implied Volatility Slope

Notes: This figure plots (binned) scatterplots of firm-level regressions of option market aggregates on $\text{CyberRisk}^{\mathbf{R}}_{\mathbf{i,t}}$. Each plot includes 100 equally-sized bins. Specifications include firm and quarter fixed effects as well as the following controls: firm size, beta, age, Tobin's Q, leverage, liquidity, intangibles / assets, and operational costs / assets.

Firm-Level Option Market Effects: Dynamics

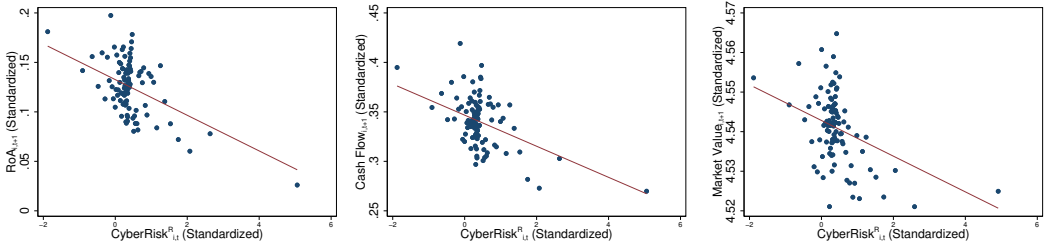


(A) Implied Volatility (B) Variance Risk Premium (C) Implied Volatility Slope

Notes: This figure plots dynamic effects of firm-level regressions of balance sheet and option market aggregates on $\text{CyberRisk}^{R}_{i,t}$. Each sub-plot shows relative quarters on the x-axis and standardized estimates with 90% confidence bands on the y-axis. Contemporaneous effects are normalized to 0. Specifications include firm and quarter fixed effects as well as the following controls: firm size, beta, age, Tobin's Q, leverage, liquidity, intangibles / assets, and operational costs / assets.

- Effects are persistent and long-lasting for all three option market variables

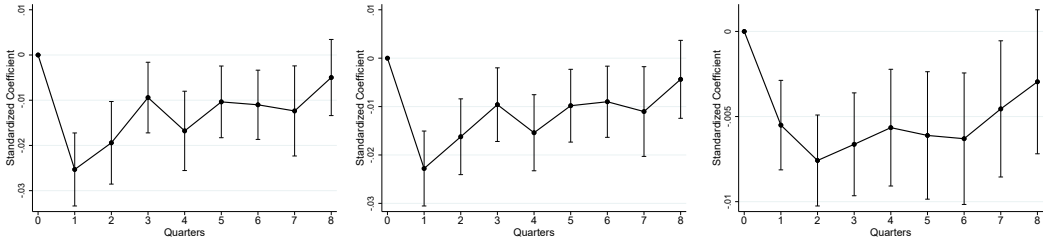
Firm-Level Economic Effects



(A) Return on Assets (B) Cash Flow Ratio (C) Market Value

Notes: This figure plots (binned) scatterplots of firm-level regressions of future (lead=1 quarter) balance sheet aggregates on $\text{CyberRisk}^{R}_{i,t}$. Each plot includes 100 equally-sized bins. Specifications include firm and quarter fixed effects as well as the following controls: firm size, beta, age, Tobin's Q, leverage, liquidity, intangibles / assets, and operational costs / assets.

Firm-Level Economic Effects: Dynamics



(A) Return on Assets (B) Cash Flow Ratio (C) Market Value

Notes: This figure plots dynamic effects of firm-level regressions of balance sheet aggregates on $\text{CyberRisk}^{\mathbf{R}}_{i,t}$. Each sub-plot shows relative quarters on the x-axis and standardized estimates with 90% confidence bands on the y-axis. Contemporaneous effects are normalized to 0. Specifications include firm and quarter fixed effects as well as the following controls: firm size, beta, age, Tobin's Q, leverage, liquidity, intangibles / assets, and operational costs / assets.

- Balance sheet effects are persistent
- Mechanism: reputational capital damage (Akey et al. 2021, Engels et al. 2022)

Sector-Level Effects

Panel A: NAICS3

Aggregation:	Equally-Weighted				Assets-Weighted			
Dependent Variable (std.):	IV	VRP	SlopeD	RoA_{t+1}	IV	VRP	SlopeD	RoA_{t+1}
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
$CyberRisk^{R}_{s,t}$ (std.)	0.024***	0.026***	0.015***	-0.019*	0.028***	0.028***	0.013**	-0.026**
	(0.009)	(0.010)	(0.005)	(0.012)	(0.009)	(0.009)	(0.006)	(0.012)
Controls	✓	✓	✓	✓	✓	✓	✓	✓
Sector FE	✓	✓	✓	✓	✓	✓	✓	✓
Country x Time FE	✓	✓	✓	✓	✓	✓	✓	✓
Level	Sector	Sector	Sector	Sector	Sector	Sector	Sector	Sector
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	14851	14850	14844	14322	14851	14850	14844	14322
R^2	0.794	0.553	0.872	0.437	0.796	0.518	0.864	0.45

Notes: Results from sector-level regressions. Specifications include industry and country x time fixed effects as well as usual controls that are aggregated to the sector-time level by averaging. Panels (A) and (B) report results for different levels of industry aggregation: 3-digit and 4-digit NAICS codes, respectively. Standard errors clustered by industry are in parentheses.

- Both option market and balance sheet effects survive sectoral aggregation.

Sector-Level Effects

Panel B: NAICS4

Aggregation:	Equally-Weighted				Assets-Weighted			
Dependent Variable (std.):	IV	VRP	SlopeD	RoA_{t+1}	IV	VRP	SlopeD	RoA_{t+1}
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
$CyberRisk^{R}_{s,t}$ (std.)	0.021***	0.018**	0.009*	-0.018**	0.019***	0.017**	0.011*	-0.024***
	(0.008)	(0.008)	(0.005)	(0.009)	(0.007)	(0.007)	(0.006)	(0.008)
Controls	✓	✓	✓	✓	✓	✓	✓	✓
Sector FE	✓	✓	✓	✓	✓	✓	✓	✓
Country x Time FE	✓	✓	✓	✓	✓	✓	✓	✓
Level	Sector	Sector	Sector	Sector	Sector	Sector	Sector	Sector
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	24829	24828	24818	24138	24829	24828	24818	24138
R^2	0.794	0.526	0.846	0.391	0.796	0.494	0.846	0.392

Notes: Results from sector-level regressions. Specifications include industry and country x time fixed effects as well as usual controls that are aggregated to the sector-time level by averaging. Panels (A) and (B) report results for different levels of industry aggregation: 3-digit and 4-digit NAICS codes, respectively. Standard errors clustered by industry are in parentheses.

- Robustness to different levels of aggregation.

Spillover Effects

	All Firms				Peer Firms			
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	IV	VRP	SlopeD	RoA_{t+1}	IV	VRP	SlopeD	RoA_{t+1}
CyberRisk (std.)	0.006**	0.016***	0.004**	-0.010**	0.013**	0.019**	0.009*	-0.023**
	(0.003)	(0.004)	(0.002)	(0.004)	(0.006)	(0.010)	(0.005)	(0.011)
Firm FE	✓	✓	✓	✓	✓	✓	✓	✓
Industry x Time FE	✓	✓	✓	✓	✓	✓	✓	✓
Firm Controls	✓	✓	✓	✓	✓	✓	✓	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	98965	98956	98875	99588	56754	56747	56716	54509
R^2	0.826	0.412	0.887	0.563	0.823	0.430	0.886	0.510

Notes: Results from regressions of firm-level outcomes on country x industry x time cyber risk exposure, constructed by averaging the firm-level $\text{CyberRisk}_{i,t}^{R}$ measure. Affected firms are firms with positive firm-level exposure. Peer firms are defined as firms with zero firm-level exposure but which belong to a country, industry, and quarter with positive exposure. Industries are defined by the 4-digit NAICS code. All specifications include the usual firm controls as well as firm and industry x time fixed effects. Every dependent and independent variable has been standardized. Standard errors are double-clustered by industry and time.

- Firm-level cyber risk exposure propagates across financial markets.

Quantifying the Global Cost of Cyber Risk

- Results: 1 std $\uparrow$ in $\text{CyberRisk}^{R}_{i,t}$ lowers future RoA by 2.5% of the std or 0.11%

Quantifying the Global Cost of Cyber Risk

- Results: 1 std $\uparrow$ in $\text{CyberRisk}^{R}_{i,t}$ lowers future RoA by 2.5% of the std or 0.11%
- The average firm in our sample has assets of about $\$25,572$M

Quantifying the Global Cost of Cyber Risk

- Results: 1 std $\uparrow$ in $\text{CyberRisk}^{R}_{i,t}$ lowers future RoA by 2.5% of the std or 0.11%
- The average firm in our sample has assets of about $\$25,572$M
- This yields a loss of income for the average firm of $\$28$ million

Quantifying the Global Cost of Cyber Risk

- Results: 1 std $\uparrow$ in $\text{CyberRisk}^{R}_{i,t}$ lowers future RoA by 2.5% of the std or 0.11%
- The average firm in our sample has assets of about $\$25,572$M
- This yields a loss of income for the average firm of $\$28$ million
- Number of unique firms in estimation sample: 2,025

Quantifying the Global Cost of Cyber Risk

- Results: 1 std $\uparrow$ in $\text{CyberRisk}^{R}_{i,t}$ lowers future RoA by 2.5% of the std or 0.11%
- The average firm in our sample has assets of about $\$25,572$M
- This yields a loss of income for the average firm of $\$28$ million
- Number of unique firms in estimation sample: 2,025
- Cost for the whole sample is $\$56,664$M **per quarter or** $\$226,576$M **per year**

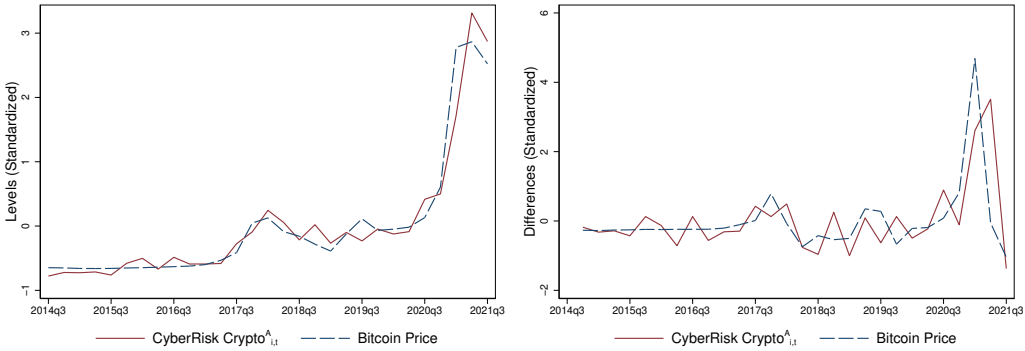
Quantifying the Global Cost of Cyber Risk

- Results: 1 std $\uparrow$ in $\text{CyberRisk}^{R}_{i,t}$ lowers future RoA by 2.5% of the std or 0.11%
- The average firm in our sample has assets of about $\$25,572$M
- This yields a loss of income for the average firm of $\$28$ million
- Number of unique firms in estimation sample: 2,025
- Cost for the whole sample is $\$56,664$M **per quarter or** $\$226,576$M **per year**
- Total cost for the actual real economy is potentially *much* higher:
  1. Private firms, or those listed not in the U.S.?
  2. Indirect costs of cyber risk (precautionary expenses, cyber insurance)?

Quantifying the Global Cost of Cyber Risk

- Results: 1 std $\uparrow$ in $\text{CyberRisk}^{R}_{i,t}$ lowers future RoA by 2.5% of the std or 0.11%
- The average firm in our sample has assets of about $\$25,572$M
- This yields a loss of income for the average firm of $\$28$ million
- Number of unique firms in estimation sample: 2,025
- Cost for the whole sample is $\$56,664$M **per quarter or** $\$226,576$M **per year**
- Total cost for the actual real economy is potentially *much* higher:
  1. Private firms, or those listed not in the U.S.?
  2. Indirect costs of cyber risk (precautionary expenses, cyber insurance)?
- Orders of magnitude consistent with other studies (Bouveret 2018, Dreyer et al. 2018)

Cyber Risk and Crypto



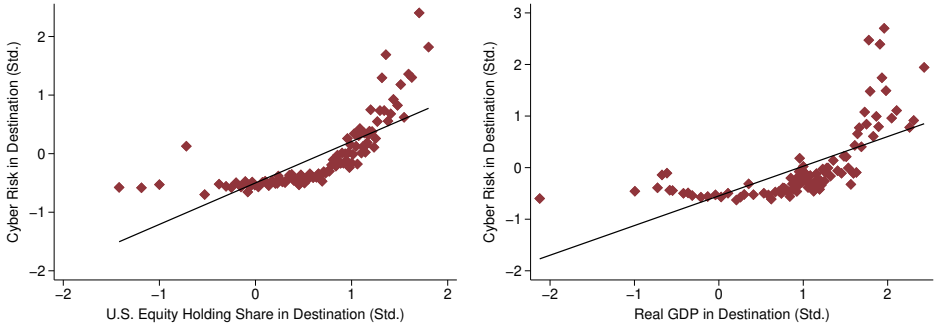
(A) Levels

(B) First Differences

Notes: This figure plots the price of Bitcoin and CyberRisk Crypto^{A}_{t}; in levels (left panel) and first differences (right panel).

- Crypto - the currency of cyber crime?

Global Cyber and Gravity Model



(A) U.S. Equity Holdings (B) GDP in Destination

Notes: This figure plots binned scatter plots and linear regression fit lines based on gravity panel regressions of $\text{CyberRisk}^{\mathbf{A}}_{\mathbf{c,t}}$ on the corresponding aggregates shown on the x-axes, as well as the time fixed effect and the usual country-level controls minus the variable on the x-axes.

- Portfolio investment from US a strong predictor of global cyber.

Additional Results and Robustness Checks

- Firm-level determinants of cyber exposure: size, beta, intangible assets, Tobin's Q

Additional Results and Robustness Checks

- Firm-level determinants of cyber exposure: size, beta, intangible assets, Tobin's Q
- Stock market effects: negative (positive) effects on stock returns (realized volatility)

Additional Results and Robustness Checks

- Firm-level determinants of cyber exposure: size, beta, intangible assets, Tobin's Q
- Stock market effects: negative (positive) effects on stock returns (realized volatility)
- Topical indices: $\text{CyberRiskInsurance}_t$ has strong predictive and economic effects

Additional Results and Robustness Checks

- Firm-level determinants of cyber exposure: size, beta, intangible assets, Tobin's Q
- Stock market effects: negative (positive) effects on stock returns (realized volatility)
- Topical indices: $\text{CyberRiskInsurance}_t$ has strong predictive and economic effects
- Robustness tests
  - Option maturities: results hold for 30- 60-, 90- (baseline), and 182-day options
  - Restricted time sample: results hold if 2002q2-2005q1 is removed
  - Recursive dictionary validation: run cyberattack predictions year-by-year
  - Asymmetry: set of terms $\tilde{\mathbb{C}}^C$ that lowers cyberattack probability has limited upside effects
  - Placebo tests: random assignment of cyber risk exposure within firms across time

Conclusion

- Novel firm-level quarterly measures of cyber risk exposure for 13,000 firms from 85 countries over 2002q1-2021q3
- Data is publically available
- Firm-level cyber risk is priced in the equity option market and affects firm balance sheet outcomes
- Cyber risk persists at the sector level and spills over to peer firms

Directions for future work

- Topical extensions and analysis: cryptocurrencies, insurance
- Calibrate economic models with our data and quantify the welfare cost of cyber risk

Appendix

Snippet 2: Target Corp

Back

Quarter	Company	$\text{CyberRisk}^{A}_{i,t}$	Text Snippet
2014q1	Target Corp	15	for those account numbers becomes less -desirable- but didnt the -breach- actually come from systems internally not necessarily coming from the; if traffic was down in the quarter presumably post the -breach- it was down pick a number like or is it; along with costs related to our recent -restructuring- and data -breach- along with small accounting and tax matters as weve worked; any -unauthorized- charges on their card accounts resulting from the -breach- we increased -fraud- detection for redcard holders and extended free; holiday merchandising and marketing plan immediately following news of the -breach- sales turned meaningfully -negative- but began to recover in january; it have -stopped- the actual theft of the credit card -data- or would it have -stopped- the personal information disclosure the; announcement that -criminals- had -gained- access to guest payment card -data- in our us stores in total fourth quarter comparable sales; invest to ensure this recovery continues beyond our efforts in -datasecurity- security and chip -enabled- technology we are applying insights from; our guests that they would have zero liability for any -unauthorized- charges on their card accounts resulting from the -breach- we; active leader in a retail industry cyber security and data -privacy- initiative in addition we are investing million in a new; the breach is and given where we are in the -breach- itd be inappropriate for me to speculate fair enough thank you so much hi thanks i have a couple questions just a quick followup on the breach costs you showed a net you got some -insurance- payments from the breach -cost- that you had is that a should we expect that or do you have any -insurance- for these potential costs whatever they may be or is that sort of a one off in the quarter and then i have a follow up just to be clear that was -insurance-; sentiment and -traffic-

Snippet 3: Solarwinds Corp

Back

Quarter	Company	$\text{CyberRisk}^{A}_{i,t}$	Text Snippet
2021q1	Solarwinds Corp	10	potential -litigation- related to sunburst how are you thinking about -software- of these liabilities and customer claims and the degree to which solarwinds might be covered by its licensing agreements thank you for the question the point you made last is the most relevant one which is much like most software companies we have covered through our enduser licensing agreements and as you mentioned sunburst is not just a solarwinds specific issue but its a broader industry issue and as you also know most software vendors unfortunately have vulnerabilities that they disclose and correct on a goforward basis and so we; expecting that headwind to continue in and like we said -breach- going to make subscription sales a priority so if anything that headwind is only going to be even a little bit stronger as we move through right but i guess what im asking is the demand impact from the breach are you expecting the demand for your subscriptions not the mix but just demand for subscriptions in general to kind of hit a bottom here nearterm and then show improvement through the year yes absolutely as weve been building out our forecast for sterling we expect the biggest impact to; anything specific to the solarwinds environment we could not find -compromise- that was idiosyncratic to the solarwinds environment and if anything both our security hygiene security posture security tools consistent with what is practiced in the industry

Snippet 4: Cisco Systems Inc

Back

Quarter	Company	$\text{CyberRisk}^{A}_{i,t}$	Text Snippet
2018q4	Cisco Systems Inc	17	-availability- solutions yesterday we expanded our collaboration offerings with a full suite of cloud calling and team collaboration tools to extend our customers onpremise investments with new hybrid solutions from the cloud to the end user these innovations include the availability of broadsoft cloud calling with -webex- teams through service providers inch -webex-board and our new portfolio of huddle room solutions with room kit mini and -webex- share in summary we had a great quarter and our opportunity has never been greater our growth continued to accelerate as we executed; single architecture to provide that capability so one of the -data- things that we talked about this week was the need to drive multidomain architectures for our customers which actually give them the ability and youre seeing us extend and connect like -policy- in the campus with -policy- in the data centers so youre seeing aci being connected into dna and our softwaredefined access technology in the campus so that we can extend -policy- you saw this week with the branch where we integrated our sdwan with our security cloud security portfolio so and i think were seeing that come through; does some pruning if you could address that and thematically -router- like to get an understanding of how you think about the sdwan products

- First example of a cybersecurity firm which has high exposure but was not attacked at the time

Snippet 6: Oracle Corp

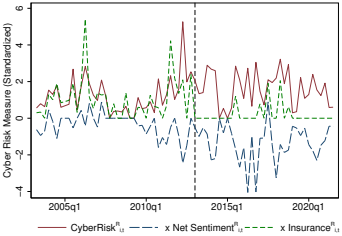
Back

Quarter	Company	$\text{CyberRisk}^{A}_{i,t}$	Text Snippet
2020q2	Oracle Corp	32	listing the additional wins i want to explain why were -computer- oracle cloud infrastructure is the worlds only secondgeneration autonomous cloud autonomous software technology the oracle autonomous database oracle autonomous linux autonomy is the defining technology that separates our gen cloud from amazons microsofts and googles generation cloud autonomous selfdriving computer systems eliminate human labor and thus eliminate human error there is nothing for humans to learn and nothing for humans to do eliminating human labor dramatically lowers the -cost- of running an autonomous system eliminating human error dramatically increases data security and system reliability all of the big data losses; and system reliability all of the big data losses at -data- were caused by human error there is no opportunity for any human error if your data is stored in an oracle autonomous system this is a very big deal the oracle autonomous database -provisions- itself configures itself encrypts the data itself patches itself and updates itself automatically scales itself up and down and continuously tunes itself as the database grows and user access patterns change and it does all of those things while the system is running theres no downtime required to patch theres no downtime required to installing new; at a count of we will this fiscal year add -firewall- gen oci regions allowing more customers to run in a public cloud without compromising data locality

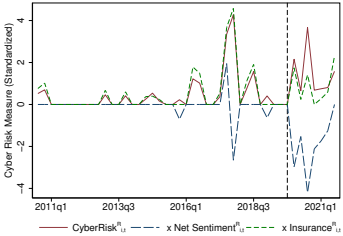
- Second example of a cybersecurity firm which has high exposure but was not attacked at the time

More Case Studies

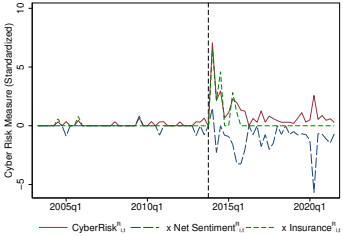
Back



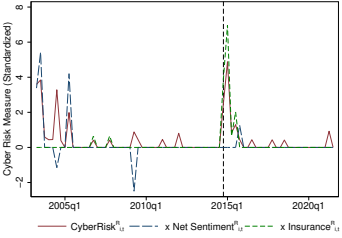
(A) Adobe



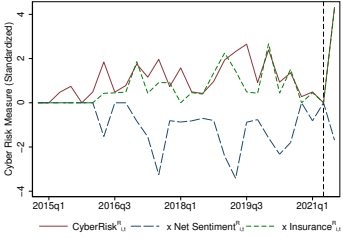
(B) First American Financial



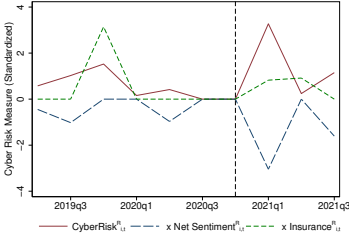
(C) Target



(D) Home Depot



(E) Alibaba



(F) SolarWinds

Predicting Cyberattacks

Back

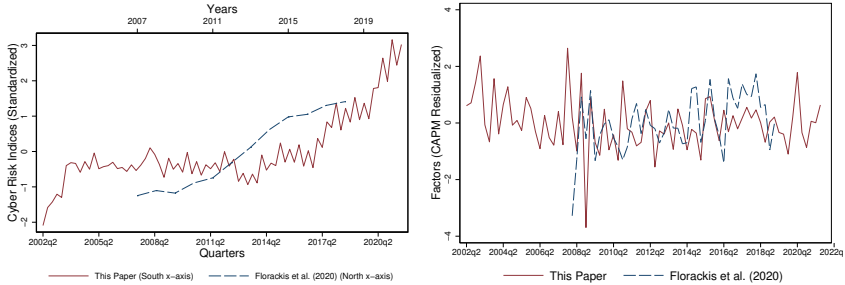
Panel B: Independent Variable - $\text{CyberRisk}^{R}_{i,t}$ (std.)

Dependent Variable:	Future Cyberattack					
	Within 1 Quarter		Within 4 Quarters		Within 8 Quarters	
	(1)	(2)	(3)	(4)	(5)	(6)
Odds Ratio	1.100***	1.132***	1.103***	1.135***	1.124***	1.159***
	(0.034)	(0.044)	(0.029)	(0.035)	(0.035)	(0.041)
Controls	No	Yes	No	Yes	No	Yes
Sector FE	Yes	Yes	Yes	Yes	Yes	Yes
Time FE	Yes	Yes	Yes	Yes	Yes	Yes
Level	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarterly	Quarterly	Quarterly	Quarterly	Quarterly	Quarterly
Clustered SE	Firm	Firm	Firm	Firm	Firm	Firm
Observations	90657	70789	98861	79112	101853	81512
Pseudo R2	0.144	0.208	0.135	0.195	0.129	0.183

Notes: predictive logit regressions of the future cyberattack indicator on the present measures of cyber risk. Panel (A) (in paper) reports results on the extensive margin, i.e for $\text{CyberRisk}^{I}_{i,t}$. Panel (B) reports results on the intensive margin, i.e for $\text{CyberRisk}^{R}_{i,t}$. Specifications include firm and time fixed effects as well as firm controls: size, beta, age, Tobin's Q, leverage, liquidity, intangibles / assets, and operational costs / assets. Standard errors clustered at the firm level are in parentheses.

Comparison to Florackis et al. (2022)

Back



(A) Indices

(B) Factors

Notes: Comparison of our measures of cyber risk with the work of Florackis et al. (2022). The left panel plots the quarterly time series of CyberRisk^{A}, developed in this paper from earnings calls (lower x-axis) and the yearly index in Florackis et al. (2022) developed from 10-K files (higher x-axis). The right panel plots quarterly factors in the two papers. Correlation between the factors is 0.39 with the p-value of 0.0186.