Risk management, firm reputation, and the impact of successful cyberattacks on target firms

Shinichi Kamiya
Nanyang Technological University

Jun-koo Kang
Nanyang Technological University

Jungmin Kim
Hong Kong Polytechnic University

Andreas Milidonis
University of Cyprus

René M. Stulz
The Ohio State University and NBER

March 12, 2020

Center For Financial Studies

FIRM

Outline

1. Motivation

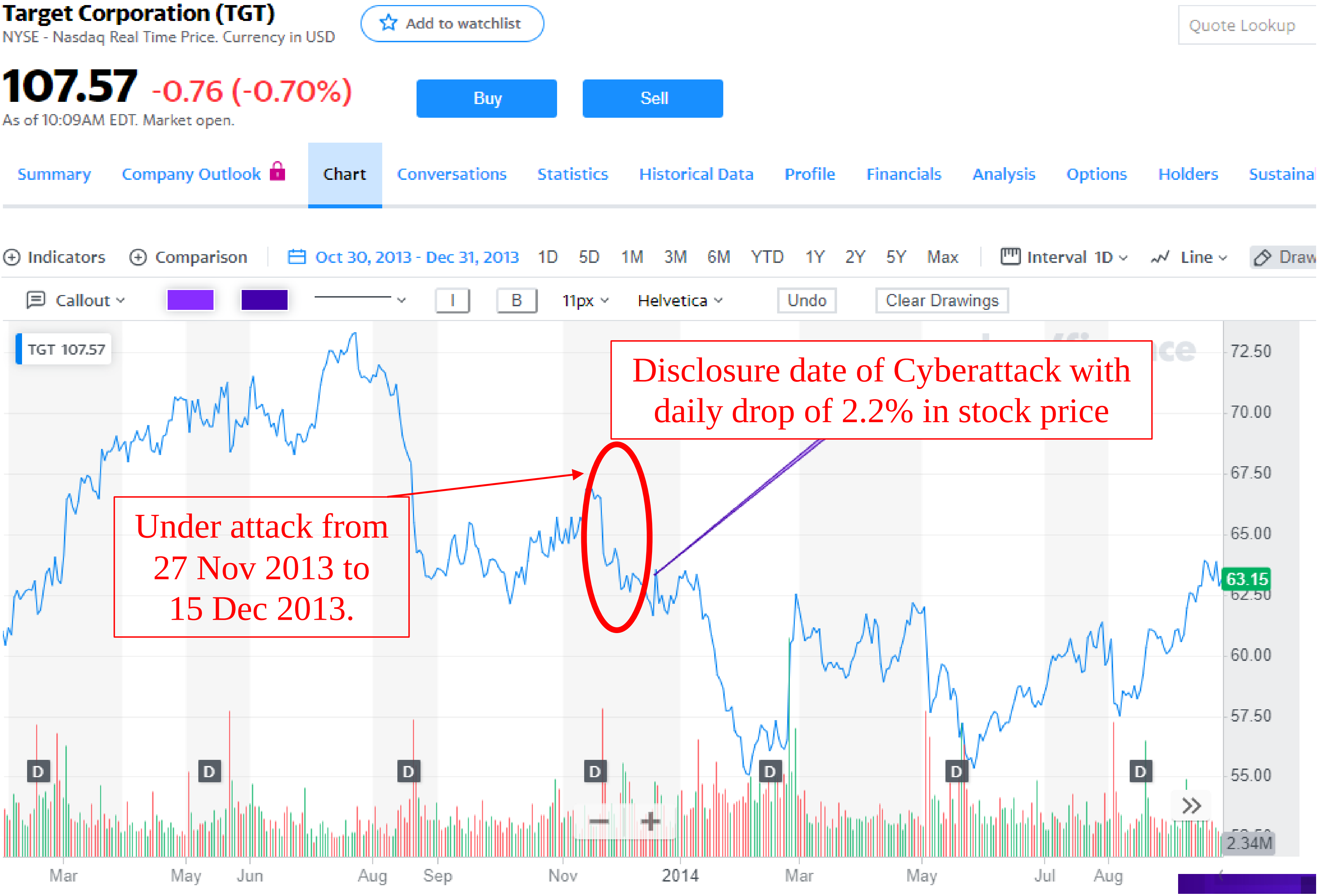
2. Research Questions

3. Sample

4. Results

5. Conclusion

2013 Target Corporation Cyberattack



Target Corporation (TGT)

NYSE - Nasdaq Real Time Price. Currency in USD

107.57 -0.76 (-0.70%)

As of 10:09AM EDT. Market open.

Oct 30, 2013 - Dec 31, 2013

Interval 1D

Disclosure date of Cyberattack with daily drop of 2.2% in stock price

Under attack from 27 Nov 2013 to 15 Dec 2013.

Anecdotal Evidence:
2013 Target Corporation Cyberattack

- Impact on Customers:
  - 70 million customers' personal information breached.
  - Names, credit/debit card number, its expiration date and CVV, address.

- Impact on firm:
  - Stock price decrease of 2.2% on the event day ($890 m).
  - Cost to upgrade IT system ($100 m).
  - Other expenses (e.g. legal costs) ($292 m).
  - Decrease in post-breach annual EBIT ($1,590 m).

Motivation (1/2)

- Cyber risk: an important source of risk for corporations.

- *Annual* worldwide cost associated with cyberattacks: $600 billion (McAfee (2018)).

- Risk practioners identify cyber risk and data security to be the most important operational risk in 2017 (Risk.net (2017)).

- More than half of the CEOs expect cybersecurity to threaten stakeholder trust over the next five years (PwC (April 2017))

Motivation (2/2)

- Despite the widespread recognition of emerging threads posed by cyber risk, we know little about:

  - which types of firms are more likely to be affected and

  - how such attacks affect target firms with respect to their operations and corporate policies.

Research Questions

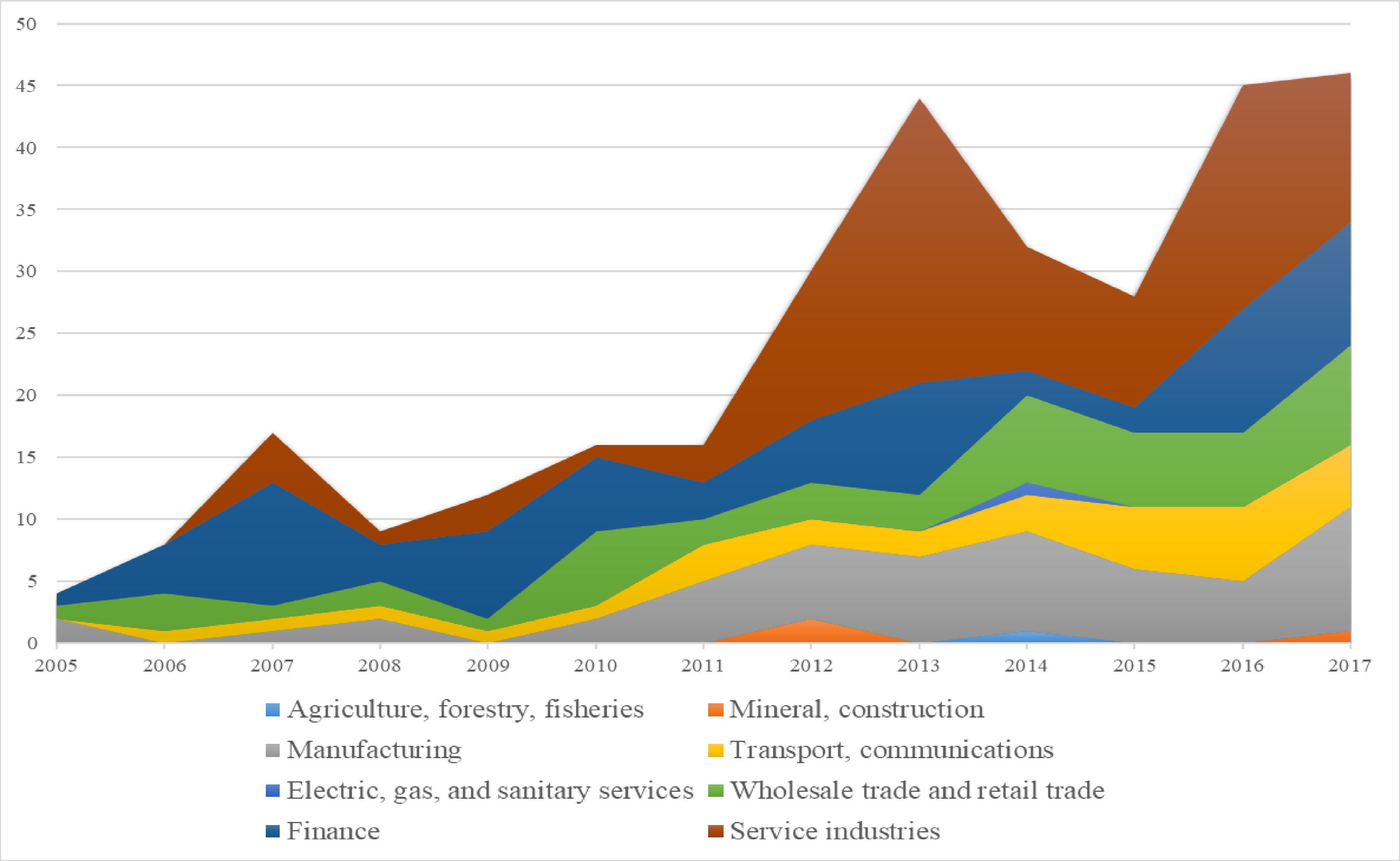
- Examine the economic implications of cyberattacks.
- Investigate which firms are more likely to be affected.
- Investigate the impact of cyber attacks on:
  - Shareholder wealth,
  - Sales growth, operating performance, and financial strength,
  - Managerial risk-taking incentives,
  - Risk management policies,
  - Reputation risk,
  - Contagion effects within the same industry.

Sample (U.S.)

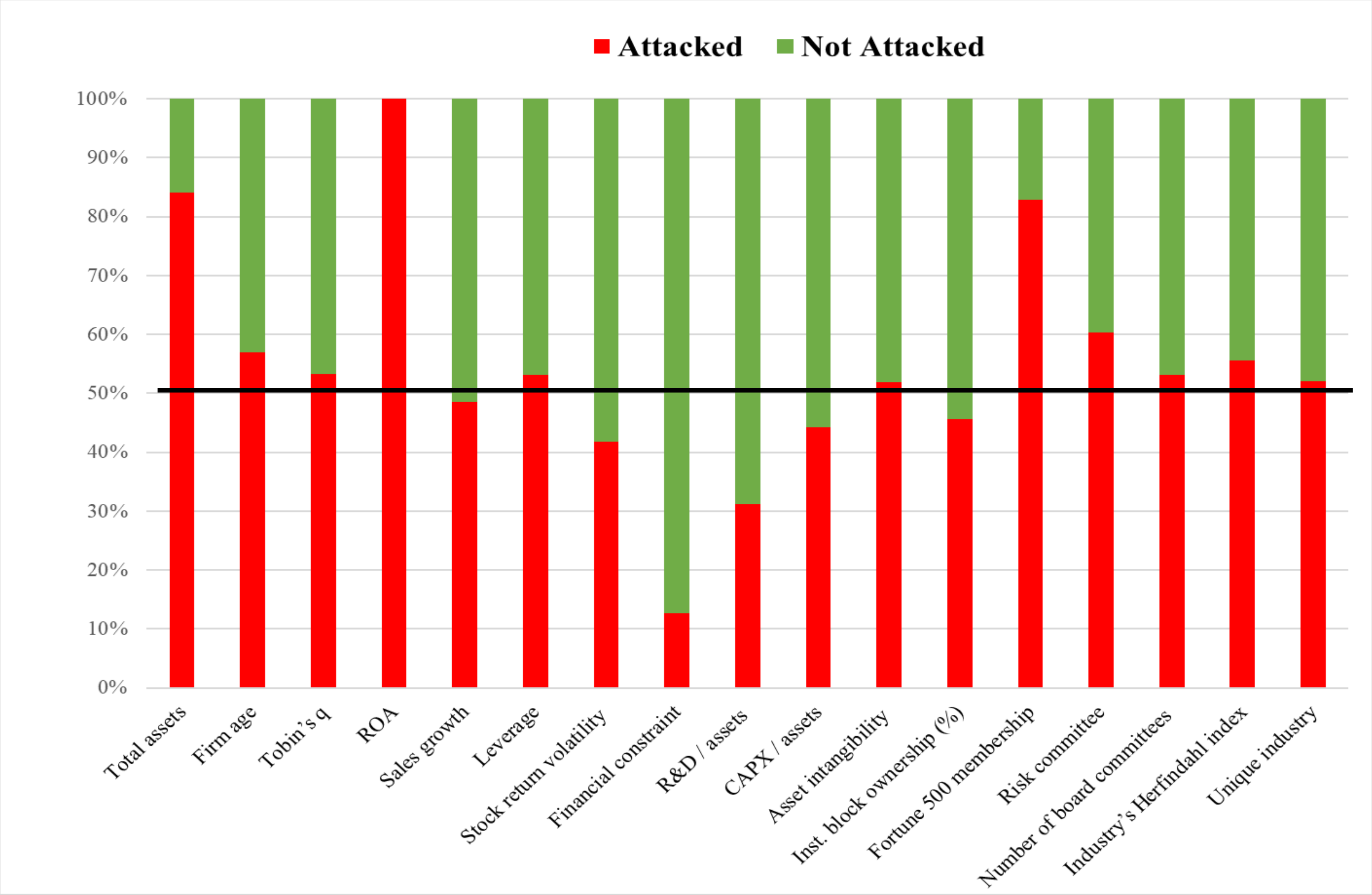
- Privacy Rights Clearinghouse database from **2005 to 2017**.
- Focus on hacking or malware-electronic entry by an outside party that caused loss of personal information (“cyberattacks”).
- Date of event cross-checked manually through newswires.
- Matched with stock prices, financial statements, executive compensation and corporate governance characteristics.

- A final sample of **307 cyberattacks** for **224 unique firms**
  - Multiple cyberattacks during the sample period: **22.8%**
  - Loss of financial information (e.g., SSN and credit card): **73.9%**

Distribution of US Cyberattacks (2005-2017) by Year and Industry



Summary statistics (2005-2017)



Results

Who is more likely to get attacked?

- Cyberattacks are more likely to occur in firms with
  - higher visibility (firm size, Fortune 500, and institutional ownership),
  - higher valuations (as measured by Tobin’s q),
  - higher Return on Assets (ROA),
  - higher asset intangibility, and
  - fewer financial constraints
  - *without* a risk committee
- And in specific industries:
  - Service industry
  - Wholesale trade
  - Transportation and communication

Table 3: Likelihood of becoming cyberattack targets

(Industry and Year FE)	Dependent variable = Cyberattack (indicator)			
	M1	M2	M3	M4
Firm size	0.203***	0.241***	0.165***	0.190***
Log (firm age)	–0.039	–0.121**	–0.105**	–0.054
Tobin’s q_{t-1}	0.063***	0.043*	0.081***	0.070***
ROA	0.843*	0.531	0.855*	0.900*
Sales growth	–0.201*	–0.172	–0.195**	–0.198*
Stock performance	–0.092	–0.099	–0.089	–0.100
Leverage	–0.292	–0.397**	–0.089	–0.144
Financially constraint (indicator)	–0.186*	–0.218*	–0.363***	–0.249**
Stock return volatility	–0.148	0.146	–0.114	–0.050
Institutional block ownership	0.004*	0.003	0.005**	0.004*
R&D / assets	–0.058	–0.029	–0.562	–0.074
CAPX / assets	0.678	1.482	1.061	0.604
Asset intangibility	0.732***	0.710***	0.686***	0.622***
Fortune 500 (indicator)	0.337***	0.245***	0.396***	0.344***
Risk committee (indicator)		–0.412***		
Number of board committees		0.039		
Industry’s Herfindahl index			0.879***	
Unique industry (indicator)			0.274**	
Industry’s Tobin’s q			0.155**	
Wholesale trade and retail trade				0.490***
Finance				–0.003
Service industries				0.544***
Transportation and communications				0.383***
Observations	45,906	40,442	54,003	48,369
Pseudo R^2	0.23	0.247	0.189	0.205

How much is the shareholder value lost?

- Many studies have tried measuring this.

- Evidence is mixed:
  - Some studies find negative stock market.
  - Others do not find reaction.

- One Reason: inaccurate disclosure/reported dates.

- To address this reason:
  - Manually confirm all events from newswires.
  - Conduct Event studies around each confirmed announcement.

How much is the shareholder value lost?

- **Stock market reaction:**
  - For the full sample,
    - Cumulative Abnormal Return around announcement (***t=0***)
      - Over (-1, 1): **-0.8%** 3-day effect
      - Over (-2, 2) : **-1.1%** 5-day effect
  - On sample of cyberattacks with loss of financial information:
    - Cumulative Abnormal Return
      - Over (-1, 1): **-1.1%** 3-day effect
      - Over (-2, 2) : **-1.5%** 5-day effect

Table 4
Cumulative Abnormal Returns (CARs) for Firms around Cyberattack Announcement Dates

	Market model				Three and four factor models			
	Value-weighted		Equally weighted		Fama-French three factor		Fama-French-Carhart four-factor	
CARs (%)	Mean	Median	Mean	Median	Mean	Median	Mean	Median
CAR (-1, 1)	−0.844***	−0.521***	−0.794***	−0.571***	−0.768***	−0.521***	−0.750***	−0.441***
CAR (-2, 2)	−1.101***	−0.810**	−1.001***	−0.768***	−1.035***	−0.546***	−1.055***	−0.511***
CAR (-5, 5)	−1.099**	−1.355***	−1.240**	−1.330***	−1.066**	−1.198**	−1.115**	−0.990***

Panel B. Comparison of CARs between cyberattacks with and without financial information loss

	Financial information loss (N=118): a		No financial information loss (N=47): b		Test of difference (a – b): *p*-value	
CARs (%)	Mean	Median	Mean	Median	*t-test*	Wilcoxon z-test
CAR (-1, 1)	–1.087***	–0.529***	–0.234	–0.311	–0.853	–0.218
CAR (-2, 2)	–1.458***	–1.136***	–0.204	–0.296	–1.254*	–0.840**
CAR (-5, 5)	–1.585**	–1.484***	0.119	–0.808	–1.704	–0.676

Does the shareholder value lost, vary by firm?

- **Yes**.

- Cross sectional analysis of (-1, 1) shows:
  - If financial Information is lost then
    - an additional **1.8% loss** (about $1.06 billion)
  - Repeated cyberattacks in one year:
    - an **additional 2.5% loss** (about $1.47 billion extra)
  - Without Board oversight:
    - an **additional 4.0% loss** (about $2.35 billion extra)

Table 4 Panel C
Cumulative Abnormal Returns (CARs) for Firms around Cyberattack Announcement Dates

(Industry and Year FE)	CAR (–1, 1)							
Independent variable	M1	M2	M3	M4	M5	M6	M7	M8
Financial information loss (indicator)	–0.018**	–0.018**	–0.014**	–0.012*	–0.017*	–0.017*	–0.047**	–0.027
Repeated cyberattacks within one year (indicator)		–0.025*	–0.018	–0.018	–0.024	–0.025	–0.021	–0.037*
Board attention to risk management (indicator)					0.040*			
State law (indicator)						–0.016		
Delay of discovery							–0.007*	
Delay of reporting								0.001
Industry’s Herfindahl index			0.03					
Unique industry (indicator)			0.003					
Industry’s Tobin’s q			–0.015**					
Transportation / communications industry (indicator)				–0.002				
Wholesale / retail trade industry (indicator)				0.011				
Finance industry (indicator)				–0.001				
Service industry (indicator)				–0.005				
Firm size		0.002	0.002	0.002	0.001	0.002	0.008	0.008*
Log (firm age)		–0.013*	–0.012**	–0.014**	–0.014*	–0.013	–0.036***	–0.031***
ROA		0.003	0.036	0.041	0.028	0.018	0.068	0.072
Leverage		–0.027*	–0.015	–0.014	–0.034**	–0.030**	–0.055	–0.026
Financial constraint (indicator)		–0.000	–0.001	–0.003	–0.000	0.001	–0.008	–0.009
Sales growth		–0.025	–0.012	–0.017	–0.026	–0.021	–0.068	–0.048
Tobin’s q		0	0	–0.001	–0.001	–0.000	0.005	–0.001
Institutional block ownership		–0.000	–0.000	–0.000	–0.000	–0.000	–0.000	0
Observations	165	165	165	162	149	151	40	67
Adj. R^2	–0.095	–0.039	0.053	0.028	–0.027	–0.057	0.257	0.232

Is market value lost, explained by *out-of-pocket* cost?

- **No.**

- For a sub-sample of 75 cyberattacks:
  - Aggregate loss in shareholder wealth $104.07 billion
  - Total out-of-pocket cost is $ 0.57 billion

  - **Excess Loss** (= Market value loss - "*out-of-pocket*"):
    - $103 billion or
    - **99% of the market value lost.**

Table 5:
Total $ market value losses, out-of-pocket costs, and excess losses.

Excess loss

Dollar loss: $ millions	A subsample of 21 cyberattacks that have a negative CAR (–1, 1) when disclosed or with subsequent post-attack event announcements and also have information about out-of-pocket available	A full sample of 75 cyberattacks that have a negative CAR (–1, 1) when disclosed or with subsequent post-attack event announcements
Aggregate dollar market value loss (mean loss, median loss)	$24,159.21 ($1,150.44, $259.08)	$104,069.59 ($1,393.89, $259.08)
Out-of-pocket cost and reputation loss (% of aggregate dollar market value loss, mean loss, median loss)		
1. Investigation and remediation costs	$535.50 (2.22%, $25.50, $0.00)	$535.50 (0.51%, $7.14, $0.00)
2. Other costs	$38.60 (0.16%, $1.84, $0.00)	$38.60 (0.04%, $0.52, $0.00)
3. Legal penalties	$613.31 (2.54%, $29.21, $0.00)	$613.31 (0.59%, $8.18, $0.00)
4. Regulatory penalties	$2.04 (0.01%, $0.10, $0.00)	$2.04 (0.00%, $0.03, $0.00)
Excess loss	$22,584.31 (93.48%, $1,075.44, $237.46)	$102,966.20 (98.94%, $1,372.88, $237.46)

How do we test **if firm policies change after a Cyberattack?**

Treatment sample

Firms experiencing:

- Cyberattack

AND

- Loss of financial information

Matched sample

Un-attacked Firms

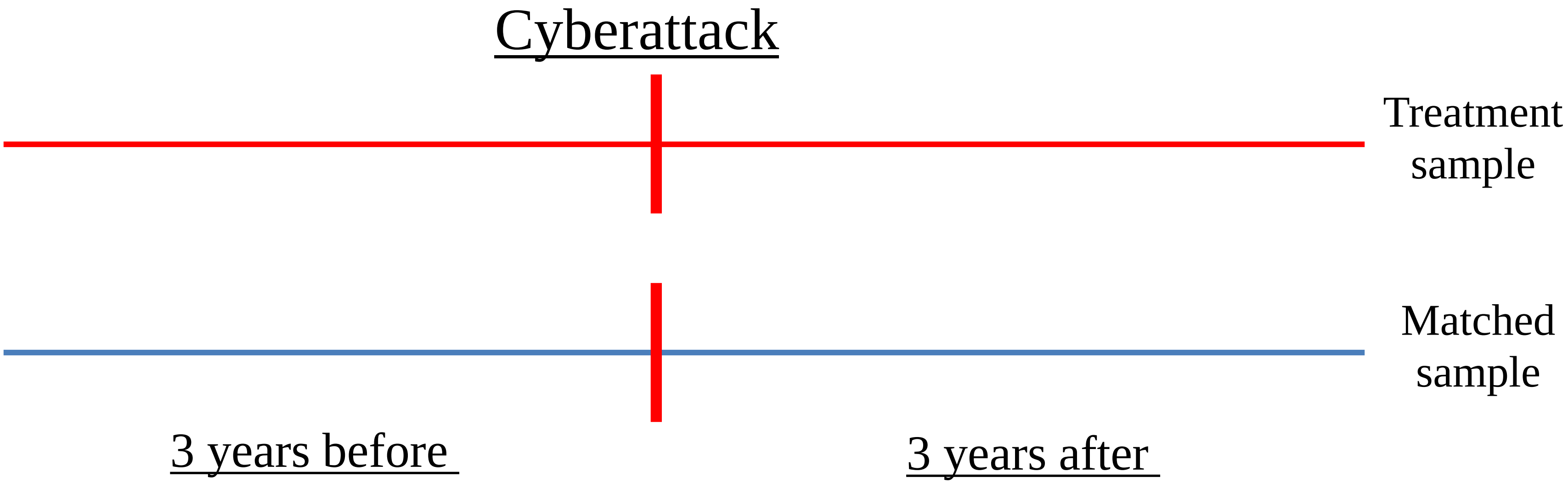
matched on:

- firm size,
- stock performance,
- stock return volatility,
- leverage, and
- the existence of an institutional blockholder
- same industry
- same fiscal year

Difference-in-Differences Analysis

Empirical Specification:

- We use annual data.
- Examine 3 years before vs. 3 years after the attack.
- For both treatment and matched sample.



Cyberattack

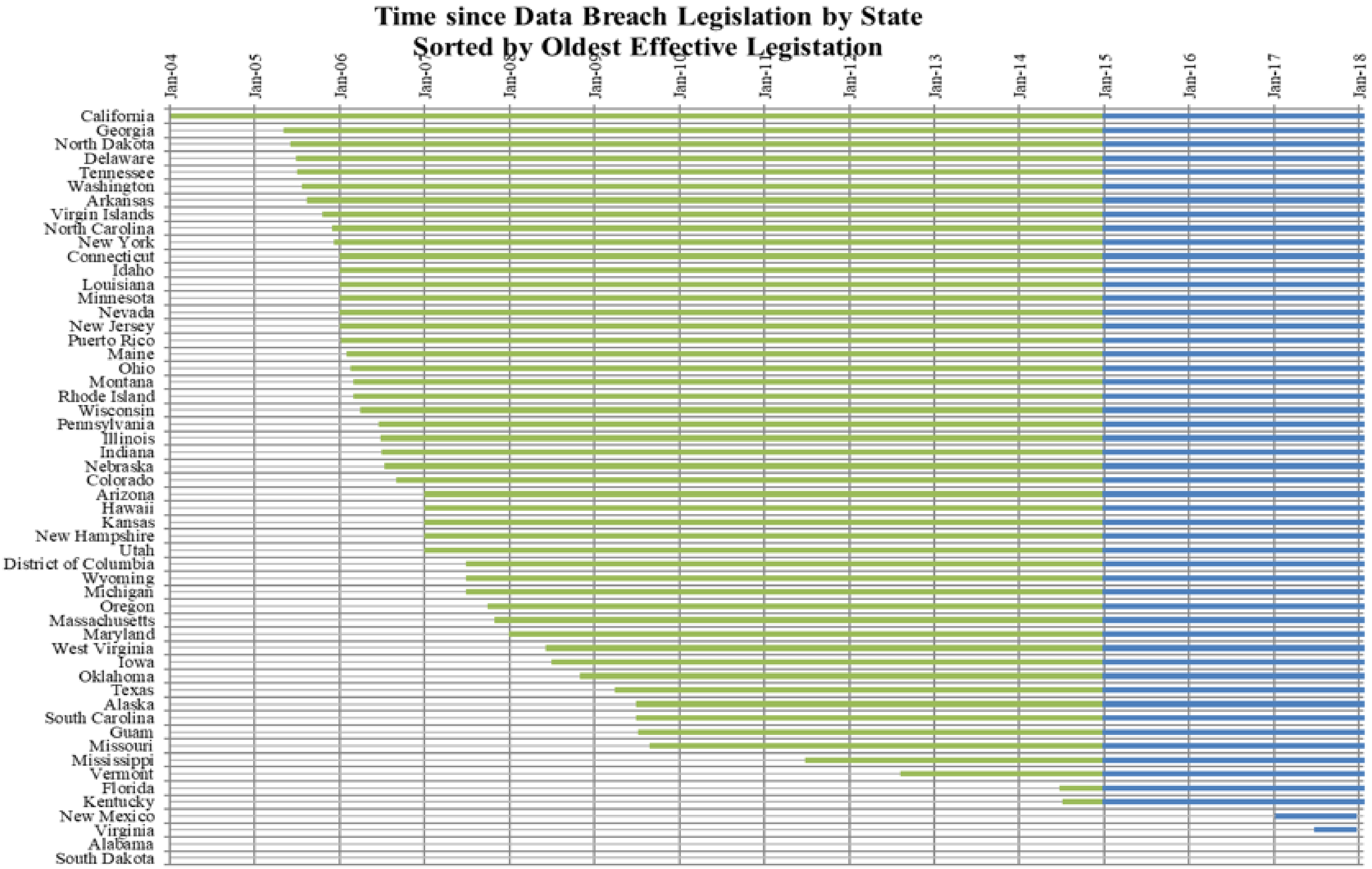
Treatment sample

Matched sample

3 years before

3 years after

Regulatory Framework



Time since Data Breach Legislation by State
Sorted by Oldest Effective Legistation

How does a cyberattack impact *Firm Performance*?

- Sales growth: about **-3.2%**
  - Majority of impact on *large firms* and firms in *retail industries*.
- Return on Assets
  - Effect only on *large firms* or *Durable goods industries*
- Cash Flow / Assets
  - Effect only on *large firms* or *Durable goods industries*

Table 6
Effects of Cyberattacks on Firms' Operating Performance

Panel B. Effects of cyberattacks on firm performance

(Industry-year FE)	Sales growth		ROA		ROE		Cash flow / assets	
Independent variable	M1	M2	M3	M4	M5	M6	M7	M8
Post (indicator) × Cyberattack (indicator)	–0.032*		–0.006		–0.021		–0.003	
Year $_t$		–0.021		–0.005		–0.019		–0.003
Year $_{t+1}$		–0.014		–0.003		–0.016		0.001
Year $_{t+2}$		–0.015		–0.003		–0.013		0.003
Firm size		–0.065		–0.020**		–0.036		–0.027**
Leverage		0.076		0.021		0.096		0.048
Tobin's q		0.064***		0.021***		0.012*		0.023***
Stock return volatility		0.135		–0.030		0.015		–0.017
Institutional block ownership		0.048		–0.008		–0.026		0.005
Observations	1,290	1,262	1,291	1,263	1,290	1,263	1,247	1,220
Adj. R^2	0.057	0.062	0.609	0.637	0.302	0.295	0.691	0.719

How does a cyberattack impact *Financial Strength*?

- S&P credit rating: about **-0.325 rating notches**

- Bankruptcy Score: increase (in probability of default)

- Net worth (= Equity/Assets): about **-3.8%**

Table 7
Effects of Cyberattacks on Firms' Financial Health

	S&P credit rating		Bankruptcy score		Net worth	
Independent variable	M1	M2	M3	M4	M5	M6
Post (indicator) × Cyberattack (indicator)	–0.325*		0.010*		–0.038***	
Year $_{t}$		–0.314***		0.003		–0.022***
Year $_{t+1}$		–0.519***		0.016*		–0.031***
Year $_{t+2}$		–0.751***		0.006		–0.038***
Control variables (ROA and those used in Panel B of Table 6)	N	Y	N	Y	N	Y
Firm fixed effects	Y	Y	Y	Y	Y	Y
Industry-year cohort fixed effects	Y	Y	Y	Y	Y	Y
Observations	788	776	1,287	1,260	1,291	1,263
Adj. R^2	0.922	0.941	0.587	0.613	0.926	0.937

How does a cyberattack impact *Risk Management policy*?

- **Increases attention to firm-wide risk management**:
  - **Board attention to risk management**: **19% more likely**
    - a board committee or the board as a whole explicitly monitors firm-wide risks
  - **Risk oversight with committee**: **16.6% more likely**
    - a specific board committee explicitly monitors firm-wide risks.
  - **Risk oversight without committee**: No effect
    - the board as a whole explicitly oversees firm-wide risks.
  - **Existence of committee with "*Risk*" in its name:** **13.6% more likely**
    - the name of a firm's board committee includes "risk" and its explicit duty involves oversight of firm-wide risk and risk management.

Table 8
Effects of Cyberattacks on Firms’ Risk Management Policy

	Board attention to risk management (indicator)		Risk oversight with committee (indicator)		Risk oversight without committee (indicator)		Existence of committee with risk name (indicator)	
Independent variable	M1	M2	M3	M4	M5	M6	M7	M8
Post (indicator) × Cyberattack (indicator)	0.190***		0.166***		0.023		0.136***	
Year $_t$		0.163***		0.139***		0.028		0.094***
Year $_{t+1}$		0.172***		0.159***		0.019		0.131***
Year $_{t+2}$		0.292***		0.258***		0.04		0.179***
Control variables (ROA and those used in Panel B of Table 6)	N	Y	N	Y	N	Y	N	Y
Firm fixed effects	Y	Y	Y	Y	Y	Y	Y	Y
Industry year-cohort fixed effects	Y	Y	Y	Y	Y	Y	Y	Y
Observations	1,126	1,102	1,126	1,102	1,126	1,102	1,126	1,102
Adj. R^2	0.687	0.728	0.812	0.826	0.857	0.864	0.761	0.763

How does a cyberattack impact *CEO Compensation*?

- CEO compensation could be affected if CEO:
  - handled the risk management poorly, or
  - did a poor job in responding to the attack, and/or
  - if attack leads to a reassessment of the firm's risk exposures and risk appetite.

How does a cyberattack impact *CEO Compensation*?

- We find the following after the cyberattack:
  - **CEO Total Pay**: No change
    - CEO **Fixed Salary Component**: No change
    - ⬇ CEO **Bonus Component**: **- 5%**
    - CEO **Equity-based Component**: No change
    - ⬆ CEO **Restricted Stock Component**: **+10.4%**
    - ⬇ CEO **Option Awards Component**: **- 6.6%**

Table 9
Effects of cyberattacks on CEO pay components (1/2)

	Log (1 + CEO total pay)		Salary / CEO total pay		Bonus / CEO total pay	
Independent variable	M1	M2	M3	M4	M5	M6
Post (indicator) × Cyberattack (indicator)	–0.063		–0.008		–0.050***	
Year $_{t}$		–0.099		–0.007		–0.043***
Year $_{t+1}$		–0.056		–0.012		–0.048***
Year $_{t+2}$		–0.114		–0.009		–0.046***
Stock performance		0.318**		–0.033		0.012
CEO-chair duality (indicator)		0.12		–0.012		–0.004
CEO age		0		–0.000		0.002
Log (CEO tenure)		–0.081		0.02		0.006
Control variables (ROA and those used in Panel B of Table 6)		Y		Y		Y
Firm fixed effects	Y	Y	Y	Y	Y	Y
Industry-year cohort fixed effects	Y	Y	Y	Y	Y	Y
Observations	1,005	985	1,005	985	1,005	985
Adj. R^2	0.567	0.594	0.565	0.587	0.409	0.432

Table 9
Effects of cyberattacks on CEO pay components (2/2)

	Equity-based compensation / CEO total pay		Restricted stock grants / CEO total pay		Option awards / CEO total pay	
Independent variable	M7	M8	M9	M10	M11	M12
Post (indicator) × Cyberattack (indicator)	0.037		0.104***		–0.066***	
Year $_{t}$		0.042		0.084***		–0.043**
Year $_{t+1}$		0.032		0.103***		–0.072***
Year $_{t+2}$		0.016		0.112***		–0.094***
Stock performance		0.03		0.048*		–0.019
CEO-chair duality (indicator)		–0.000		0.033		–0.036
CEO age		0.001		0.003		–0.003
Log (CEO tenure)		–0.060***		–0.047**		–0.012
Control variables (ROA and those used in Panel B of Table 6)		Y		Y		Y
Firm fixed effects	Y	Y	Y	Y	Y	Y
Industry-year cohort fixed effects	Y	Y	Y	Y	Y	Y
Observations	1,005	985	1,005	985	1,005	985
Adj. R^2	0.459	0.492	0.519	0.547	0.594	0.616

How does a cyberattack impact *CEO Compensation and Risk-Taking*?

Results support view that cyberattacks:

- **Increase** boards' assessment of target firm risk exposures

  &

- **Decrease** their risk appetite.

Do cyberattacks generate *spillover effects within the same industry*?

- **Yes.** We observe loss in shareholder wealth in firms in the same industry at the time of the cyberattack.

- **Stock market reaction:**
  - Cumulative Abnormal Return

– Over (-1, 1):	**-0.37%**	3-day effect
– Over (-2, 2) :	**-0.62%**	5-day effect
– Over (-5, 5) :	**-0.92%**	11-day effect

Do cyberattacks generate *spillover effects within the same industry*?

- Analysing stock market reaction by firm characteristics shows:
  - **More negative** reaction if attack was:
    - on finance industry and with loss of financial information.
  - **Less negative reaction** if attack was:
    - a repeated one and in a highly competitive industry.

Table 11
Cumulative abnormal returns (CARs) for portfolios of industry competitors around cyberattack announcement dates

Panel A. Univariate analysis

	Value-weighted portfolio		Equal-weighted portfolio	
CARs (%)	Mean	Median	Mean	Median
CAR (–1, 1)	–0.372***	–0.174***	–0.347***	–0.121***
CAR (–2, 2)	–0.622***	–0.307***	–0.555***	–0.196***
CAR (–5, 5)	–0.920***	–0.428***	–0.988***	–0.272***

Panel B. OLS regressions of CARs (–1, 1) for the value-weighted portfolio of individual industry peer firms

Independent variable	M1	M2	M3
Attacked firm CAR (–1, 1)	0.141***	0.140***	0.139***
Financial information loss (indicator): **a**	0.004	0.002	0.002
Repeated cyberattack within one year (indicator): **b**	–0.000	–0.002	–0.008**
Returns correlation	–0.013	–0.009	–0.010
Log (average price)	–0.000	0.003	0.003*
Finance industry (indicator): **c**		0.007	–0.004
High competition (indicator): **d**		0	0
Unique industry (indicator)		0.002	0.002
Industry's Tobin's q		0.002	0.001
a × c		–0.012*	
b × d			0.011**
Firm-level characteristics (those used in Panel C of Table 4)	Y	Y	Y
Observations	146	146	146
Adj. R^2	0.136	0.118	0.117

Conclusions (1/2)

- We investigate which firms are more likely to suffer from a cyberattack and how firms are affected by cyberattacks.
- Successful targets are more visible and more highly valued, have more intangible assets, and their boards pay less attention to risk management prior to the attack.
- Attacked firms in which personal financial information is lost suffer a substantial loss in equity value.
- Larger firms and firms in retail industries experience a drop in sales growth and firms in durable goods industries suffer a decline in ROA and cash flow in the post-attack period.

Conclusions (2/2)

- Affected firms increase board oversight of firm risk.
- Firms cut their bonuses and reduce the risk-taking incentives of their CEOs by replacing the payments of stock options with those of restricted stocks.
- Attacks affect companies in the same industry: more negatively if the attack was in finance and with loss of financial information; less negatively if target was struck repeatedly in a highly competitive industry.
- Overall, our evidence is consistent with the hypothesis that a cyberattack leads to a reassessment by the board of the firm's risk exposures and risk appetite.

Thank you!

- The article is forthcoming in the *Journal of Financial Economics* and can be accessed here: LINK

- For more information:

Email:	Andreas.Milidonis@ucy.ac.cy
Office:	+357 22 89 3626
Web:	http://amilidonis.com/