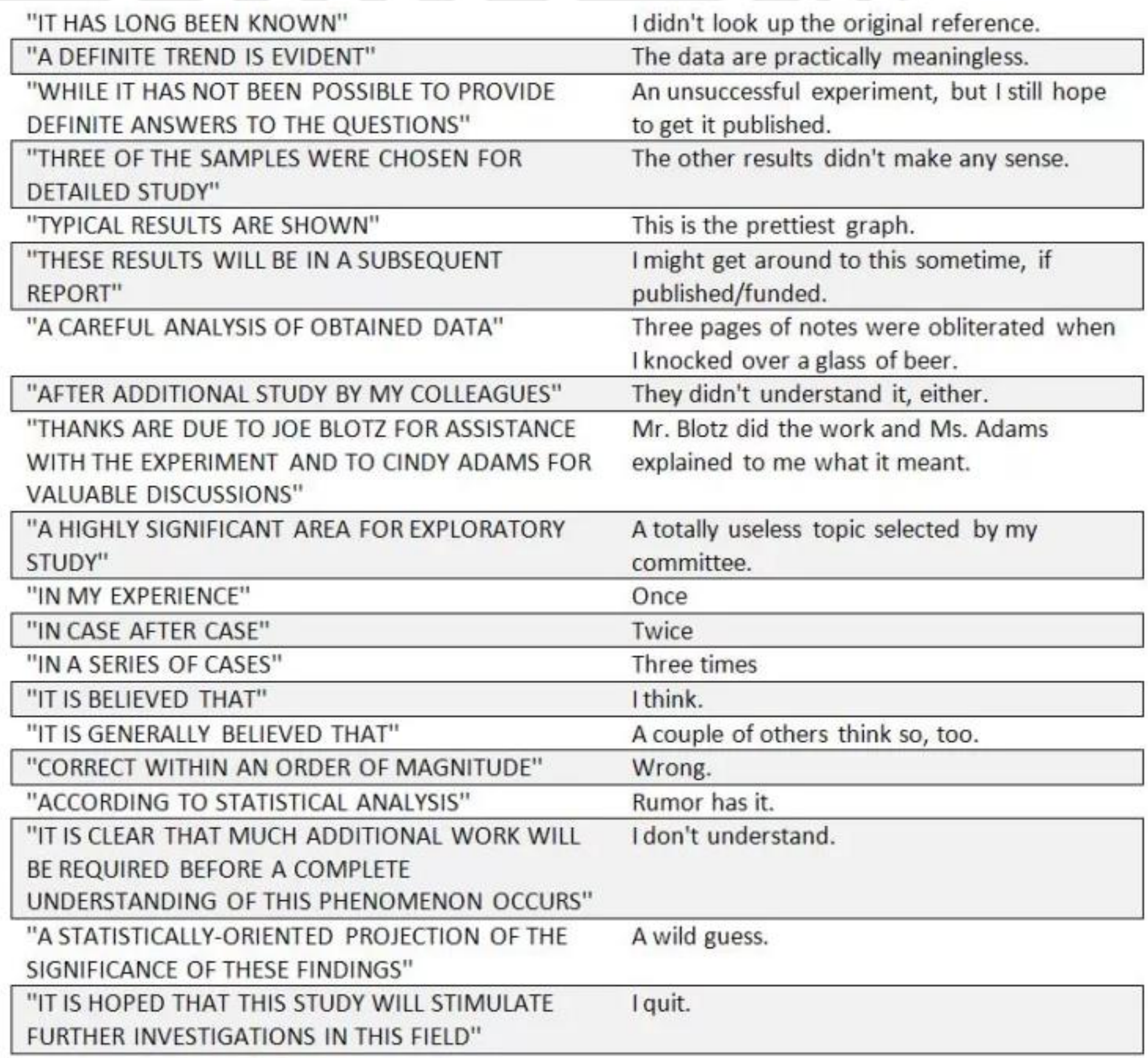
RUTGERS
Rutgers Business School
Newark and New Brunswick

41th World Continuous Auditing & Reporting Symposium
University of Huelva, Spain
November 9-10, 2017

Cybersecurity Risk Disclosure and Cybersecurity Disclosure Guidance

He Li (Southwestern University of Finance and Economics, China)
Won Gyun No (Rutgers Business School)
Tawei (David) Wang (DePaul University)
Miklos A. Vasarhelyi (Rutgers Business School)

A TRANSLATION OF COMMON SCIENTIFIC RESEARCH PHRASES!



"IT HAS LONG BEEN KNOWN"	I didn't look up the original reference.
"A DEFINITE TREND IS EVIDENT"	The data are practically meaningless.
"WHILE IT HAS NOT BEEN POSSIBLE TO PROVIDE DEFINITE ANSWERS TO THE QUESTIONS"	An unsuccessful experiment, but I still hope to get it published.
"THREE OF THE SAMPLES WERE CHOSEN FOR DETAILED STUDY"	The other results didn't make any sense.
"TYPICAL RESULTS ARE SHOWN"	This is the prettiest graph.
"THESE RESULTS WILL BE IN A SUBSEQUENT REPORT"	I might get around to this sometime, if published/funded.
"A CAREFUL ANALYSIS OF OBTAINED DATA"	Three pages of notes were obliterated when I knocked over a glass of beer.
"AFTER ADDITIONAL STUDY BY MY COLLEAGUES"	They didn't understand it, either.
"THANKS ARE DUE TO JOE BLOTZ FOR ASSISTANCE WITH THE EXPERIMENT AND TO CINDY ADAMS FOR VALUABLE DISCUSSIONS"	Mr. Blotz did the work and Ms. Adams explained to me what it meant.
"A HIGHLY SIGNIFICANT AREA FOR EXPLORATORY STUDY"	A totally useless topic selected by my committee.
"IN MY EXPERIENCE"	Once
"IN CASE AFTER CASE"	Twice
"IN A SERIES OF CASES"	Three times
"IT IS BELIEVED THAT"	I think.
"IT IS GENERALLY BELIEVED THAT"	A couple of others think so, too.
"CORRECT WITHIN AN ORDER OF MAGNITUDE"	Wrong.
"ACCORDING TO STATISTICAL ANALYSIS"	Rumor has it.
"IT IS CLEAR THAT MUCH ADDITIONAL WORK WILL BE REQUIRED BEFORE A COMPLETE UNDERSTANDING OF THIS PHENOMENON OCCURS"	I don't understand.
"A STATISTICALLY-ORIENTED PROJECTION OF THE SIGNIFICANCE OF THESE FINDINGS"	A wild guess.
"IT IS HOPED THAT THIS STUDY WILL STIMULATE FURTHER INVESTIGATIONS IN THIS FIELD"	I quit.

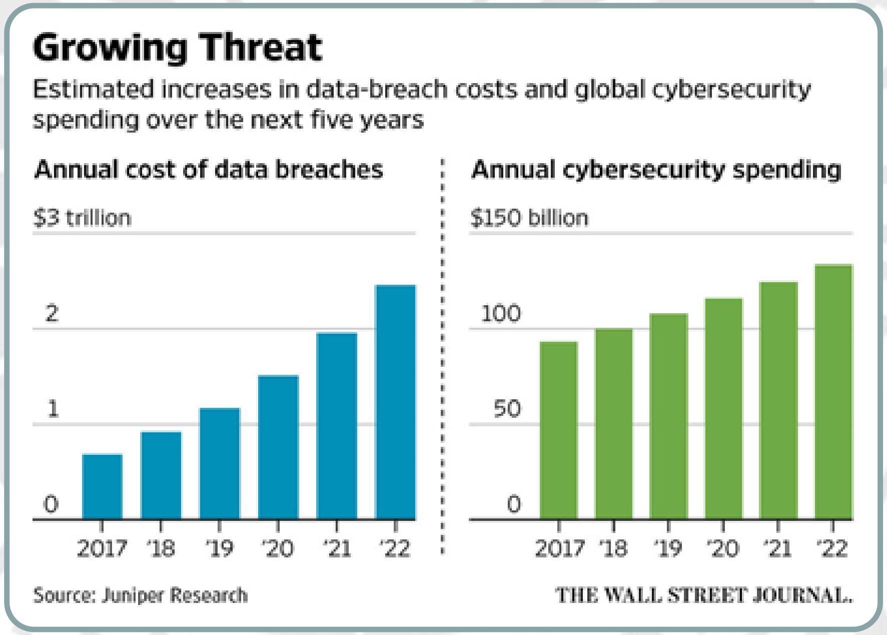
RUTGERS
Rutgers Business School
Newark and New Brunswick

AGENDA

- Research Background and Hypotheses
- Research Design and Sample Selection Procedure
- Results and Additional Tests
- Concluding Remarks

RESEARCH BACKGROUND

❖ Cybersecurity is becoming a global concern.

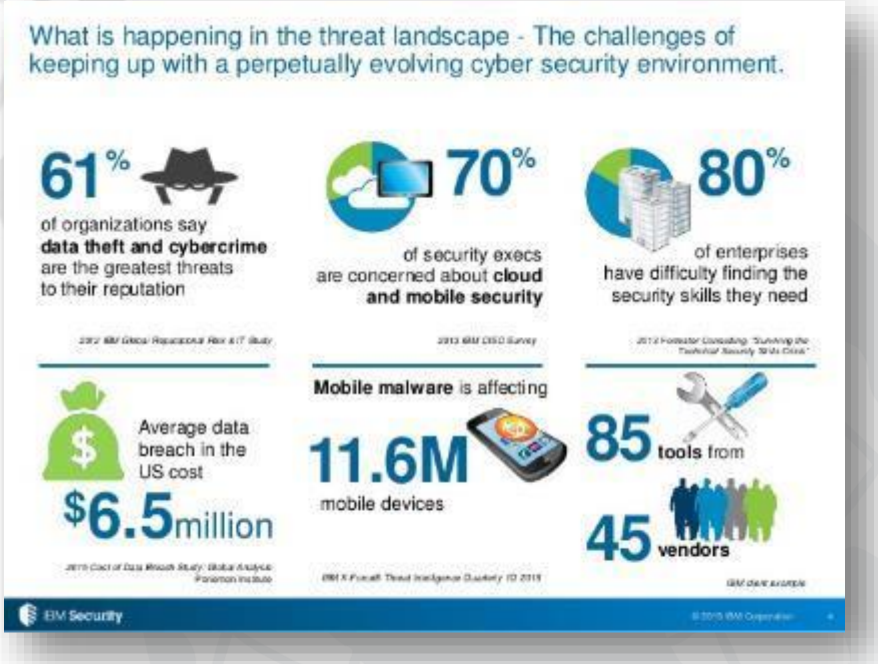


Growing Threat

Estimated increases in data-breach costs and global cybersecurity spending over the next five years

Source: Juniper Research

THE WALL STREET JOURNAL.



What is happening in the threat landscape - The challenges of keeping up with a perpetually evolving cyber security environment.

61% of organizations say **data theft and cybercrime** are the greatest threats to their reputation

2012 IBM Global Reputational Risk & IT Study

70% of security execs are concerned about **cloud and mobile security**

2013 IBM CISO Survey

80% of enterprises have difficulty finding the security skills they need

2012 Forrester Consulting: "Surviving the Technical Security Skills Crisis"

Average data breach in the US cost **$6.5million**

2015 Cost of Data Breach Study: Global Analysis Ponemon Institute

Mobile malware is affecting **11.6M** mobile devices

IBM X-Force Threat Intelligence Quarterly 1Q 2015

85 tools from **45 vendors**

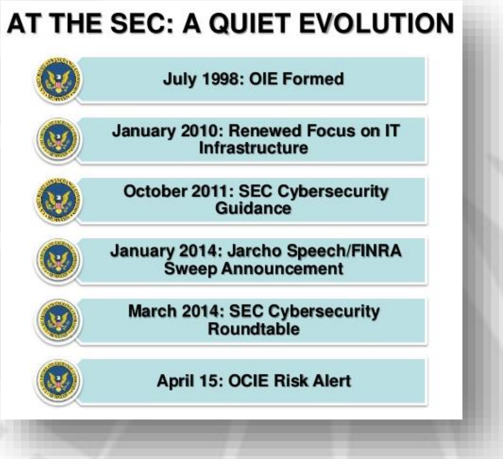
IBM client example

IBM Security

© 2015 IBM Corporation

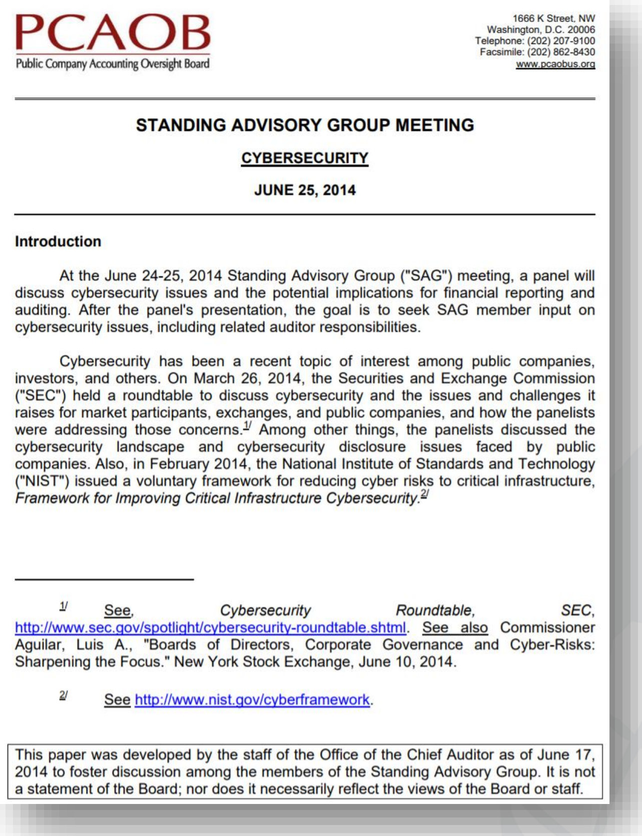
RESEARCH BACKGROUND

- ❖ Cybersecurity is becoming a global concern.
- ❖ Regulators have displayed concerns.



AT THE SEC: A QUIET EVOLUTION

- July 1998: OIE Formed
- January 2010: Renewed Focus on IT Infrastructure
- October 2011: SEC Cybersecurity Guidance
- January 2014: Jarcho Speech/FINRA Sweep Announcement
- March 2014: SEC Cybersecurity Roundtable
- April 15: OCIE Risk Alert



PCAOB
Public Company Accounting Oversight Board

1666 K Street, NW
Washington, D.C. 20006
Telephone: (202) 207-9100
Facsimile: (202) 862-8430
www.pcaobus.org

STANDING ADVISORY GROUP MEETING

CYBERSECURITY

JUNE 25, 2014

Introduction

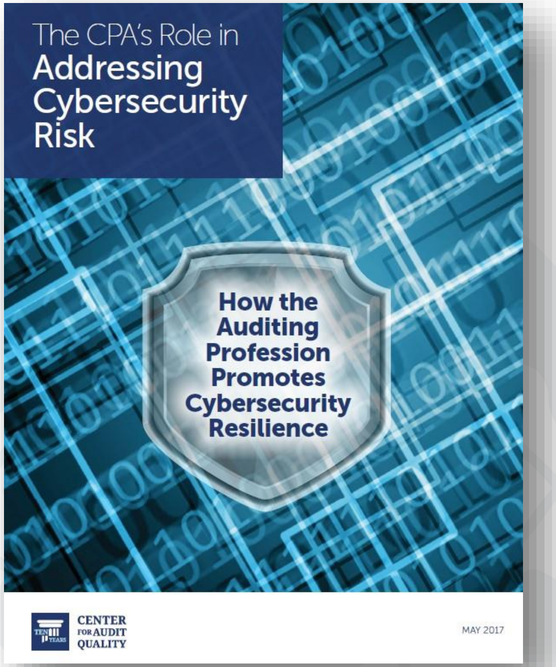
At the June 24-25, 2014 Standing Advisory Group ("SAG") meeting, a panel will discuss cybersecurity issues and the potential implications for financial reporting and auditing. After the panel's presentation, the goal is to seek SAG member input on cybersecurity issues, including related auditor responsibilities.

Cybersecurity has been a recent topic of interest among public companies, investors, and others. On March 26, 2014, the Securities and Exchange Commission ("SEC") held a roundtable to discuss cybersecurity and the issues and challenges it raises for market participants, exchanges, and public companies, and how the panelists were addressing those concerns.[1/] Among other things, the panelists discussed the cybersecurity landscape and cybersecurity disclosure issues faced by public companies. Also, in February 2014, the National Institute of Standards and Technology ("NIST") issued a voluntary framework for reducing cyber risks to critical infrastructure, *Framework for Improving Critical Infrastructure Cybersecurity*.[2/]

[1/] See, *Cybersecurity Roundtable*, SEC, http://www.sec.gov/spotlight/cybersecurity-roundtable.shtml. See also Commissioner Aguilar, Luis A., "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus." New York Stock Exchange, June 10, 2014.

[2/] See http://www.nist.gov/cyberframework.

This paper was developed by the staff of the Office of the Chief Auditor as of June 17, 2014 to foster discussion among the members of the Standing Advisory Group. It is not a statement of the Board; nor does it necessarily reflect the views of the Board or staff.



The CPA's Role in
Addressing Cybersecurity Risk

How the Auditing Profession Promotes Cybersecurity Resilience

TEN YEARS CENTER FOR AUDIT QUALITY

MAY 2017

RESEARCH BACKGROUND

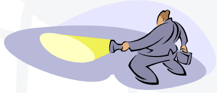
- On June 29, 2005, the SEC mandated firms to describe their material risks in Item 1A of 10-K.
- The SEC's Division of Corporation Finance issued a disclosure guidance regarding cybersecurity in 2011.
  - To assist firms in assessing what, if any, disclosures should be provided related to cybersecurity risks and cyber incidents.
  - The SEC has issued comment letters to several firms pointing out the inadequacies of their cybersecurity risk disclosures by referring to the guidance.
  - The guidance is becoming a de facto ruling (Grant and Grant, 2014).
- Cybersecurity risk disclosures have been criticized by practitioners and academics.
  - Firms use boilerplate language every year (Bennett, 2015).
  - The disclosure guidance is vague, similar across industries that will bring little information to the market.(Ferraro 2013)
- The purpose of this study is to investigate the informativeness of cyber risk disclosure (i.e., the ability to help stakeholders assess the probability of future cyber incidents) in terms of presence and content.

SUMMARY OF FINDINGS

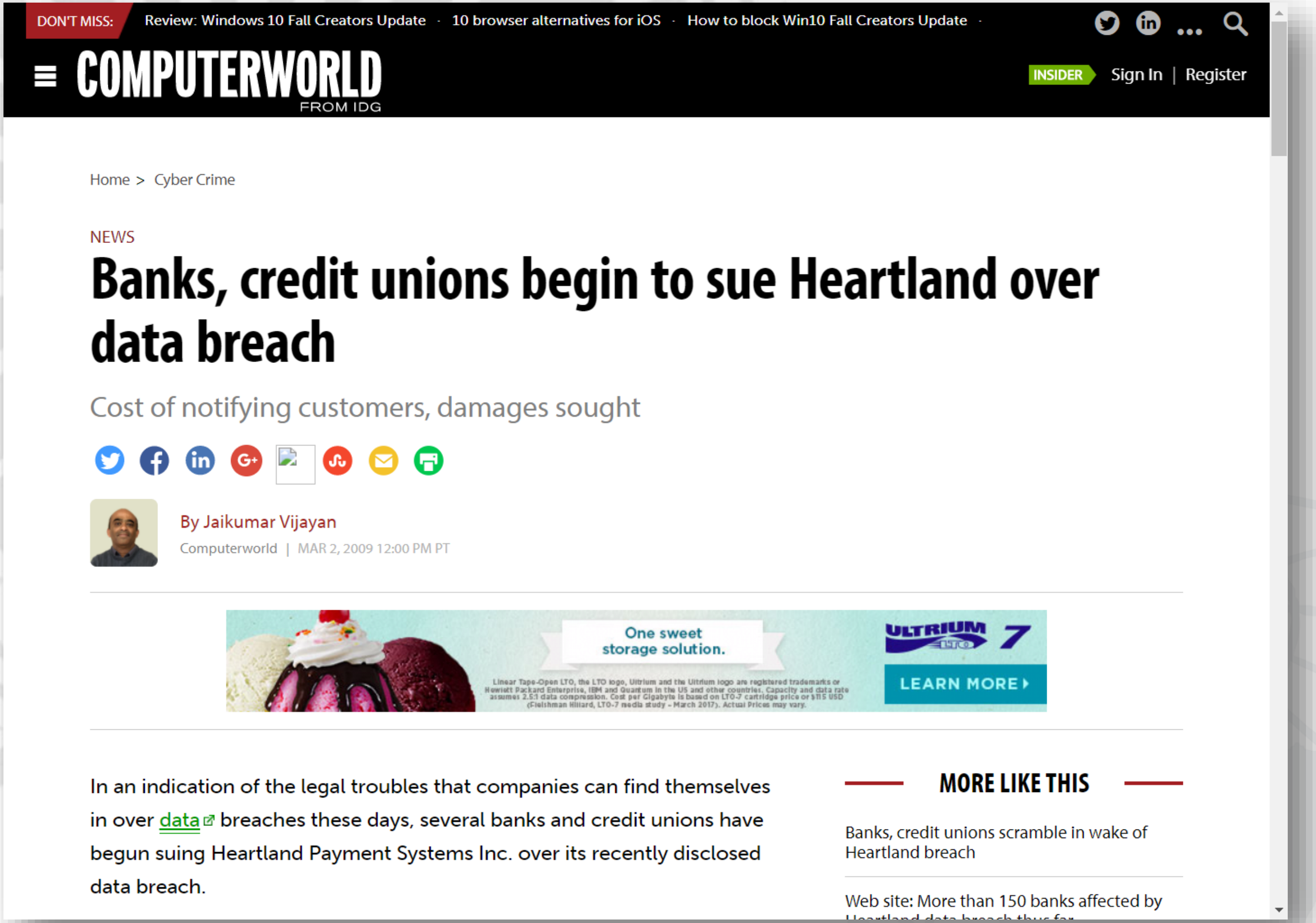
- Both the presence and the content of cyber risk disclosure are associated with subsequent cyber incidents, indicating that cyber risk disclosure is informative.
- There is a substantial increase in the percentage of firms that disclose cyber risks following the SEC's disclosure guidance.
- The presence of cyber risk disclosure is no longer associated with subsequent cyber incidents in the post-guidance period.
- Fail to find a significant association between firm-specific disclosure and cyber incidents.
- Market participants only utilize the presence of cyber risk disclosures, but not by the content of the disclosures.
- Business disruption and financial performance are the two major concerns of firms when they encounter cybersecurity issues.
- There is a growing concern regarding reputation damage and loss of intellectual property due to cyber incidents.

HYPOTHESIS

- The disclosure literature suggests that managers have incentives to disclose favorable information and withhold negative information (Beyer, Cohen, Lys, & Walther, 2010; Verrecchia, 2001).
- However, they may face legal penalties for not disclosing such information. Litigation costs could be high enough to motivate disclosures of bad news (Skinner, 1994).
- Consistent with this view, recent studies document that risk factor disclosures are generally informative (Campbell et al., 2014; Hope et al., 2016; Kravet & Muslu, 2013).
- Lawsuits may be filed if a material cyber incident happens, but the firm fails to alert the investors about the risk in advance.



HYPOTHESIS



DON'T MISS: Review: Windows 10 Fall Creators Update · 10 browser alternatives for iOS · How to block Win10 Fall Creators Update ·

COMPUTERWORLD FROM IDG

INSIDER Sign In | Register

Home > Cyber Crime

NEWS

Banks, credit unions begin to sue Heartland over data breach

Cost of notifying customers, damages sought

By Jaikumar Vijayan

Computerworld | MAR 2, 2009 12:00 PM PT

In an indication of the legal troubles that companies can find themselves in over data breaches these days, several banks and credit unions have begun suing Heartland Payment Systems Inc. over its recently disclosed data breach.

MORE LIKE THIS

Banks, credit unions scramble in wake of Heartland breach

Web site: More than 150 banks affected by Heartland data breach thus far

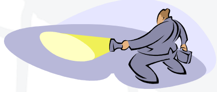
RUTGERS

Rutgers Business School
Newark and New Brunswick

HYPOTHESIS

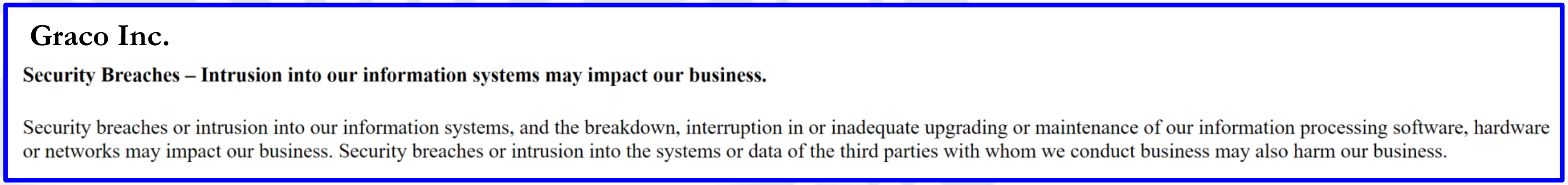
- The disclosure literature suggests that managers have incentives to disclose favorable information and withhold negative information (Beyer, Cohen, Lys, & Walther, 2010; Verrecchia, 2001).
- However, they may face legal penalties for not disclosing such information. Litigation costs could be high enough to motivate disclosures of bad news (Skinner, 1994).
- Consistent with this view, recent studies document that risk factor disclosures are generally informative (Campbell et al., 2014; Hope et al., 2016; Kravet & Muslu, 2013).
- Lawsuits may be filed if a material cyber incident happens, but the firm fails to alert the investors about the risk in advance (e.g., Heartland Payment Systems).
- Thus, we expect that firms tend to provide cyber risk disclosure when they deem the risk as a material matter.

H1. *The presence of cyber risk disclosure is positively associated with the likelihood of subsequent cyber incident.*



RUTGERS
Rutgers Business School
Newark and New Brunswick

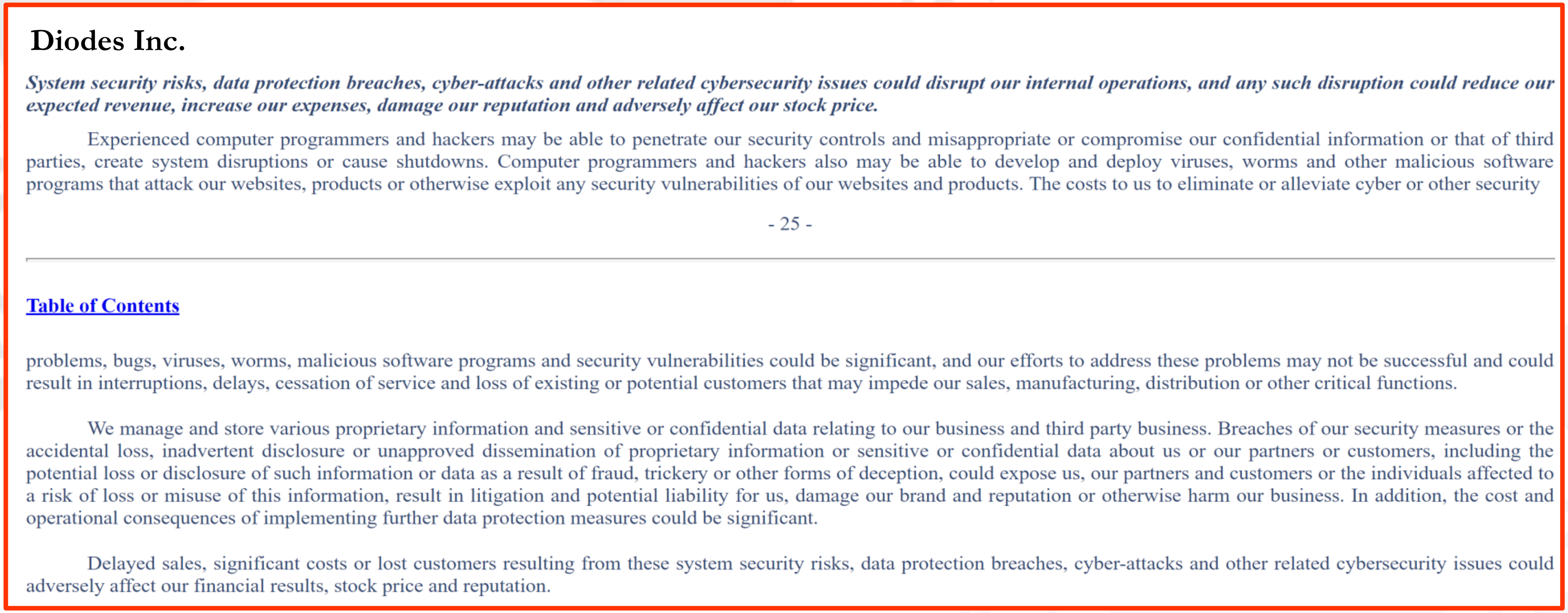
HYPOTHESIS



Graco Inc.

Security Breaches – Intrusion into our information systems may impact our business.

Security breaches or intrusion into our information systems, and the breakdown, interruption in or inadequate upgrading or maintenance of our information processing software, hardware or networks may impact our business. Security breaches or intrusion into the systems or data of the third parties with whom we conduct business may also harm our business.



Diodes Inc.

System security risks, data protection breaches, cyber-attacks and other related cybersecurity issues could disrupt our internal operations, and any such disruption could reduce our expected revenue, increase our expenses, damage our reputation and adversely affect our stock price.

Experienced computer programmers and hackers may be able to penetrate our security controls and misappropriate or compromise our confidential information or that of third parties, create system disruptions or cause shutdowns. Computer programmers and hackers also may be able to develop and deploy viruses, worms and other malicious software programs that attack our websites, products or otherwise exploit any security vulnerabilities of our websites and products. The costs to us to eliminate or alleviate cyber or other security

- 25 -

Table of Contents

problems, bugs, viruses, worms, malicious software programs and security vulnerabilities could be significant, and our efforts to address these problems may not be successful and could result in interruptions, delays, cessation of service and loss of existing or potential customers that may impede our sales, manufacturing, distribution or other critical functions.

We manage and store various proprietary information and sensitive or confidential data relating to our business and third party business. Breaches of our security measures or the accidental loss, inadvertent disclosure or unapproved dissemination of proprietary information or sensitive or confidential data about us or our partners or customers, including the potential loss or disclosure of such information or data as a result of fraud, trickery or other forms of deception, could expose us, our partners and customers or the individuals affected to a risk of loss or misuse of this information, result in litigation and potential liability for us, damage our brand and reputation or otherwise harm our business. In addition, the cost and operational consequences of implementing further data protection measures could be significant.

Delayed sales, significant costs or lost customers resulting from these system security risks, data protection breaches, cyber-attacks and other related cybersecurity issues could adversely affect our financial results, stock price and reputation.

HYPOTHESIS

- Practitioners, regulators, and academics have expressed concerns that cybersecurity risk disclosures may be boilerplate (Bennett, 2015; Hilary et al., 2017)

- If the concern is true, the content of cyber risk disclosure is not likely to be associated with the likelihood of reported future cyber incidents.

- On the other hand, Campbell et al. (2014) show that the level of risk determines the amount of disclosure firms devote to address that risk. Similarly, Filzen (2015) argues that the more discussions of potential negative outcomes, the greater the likelihood of the negative event.

- If cyber risk disclosure is informative, firms facing higher cyber risks are more likely to devote a greater portion of the disclosures to describe their cyber risks.

H2. *The content of cyber risk disclosure is positively associated with the likelihood of subsequent cyber incident.*

HYPOTHESIS

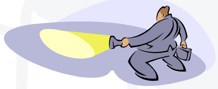
- Prior studies indicate that changes in risk factor disclosures are associated with abnormal returns surrounding the release date, information asymmetry, analyst forecast dispersion, and risk perceptions (Campbell, Chen, Dhaliwal, Lu & Steele, 2014; Filzen, 2015; Hope, Hu & Lu, 2016; Kravet & Muslu, 2013).

- However, such studies examine risk factor disclosure at the aggregate level rather than at the individual risk factor level. It is ex-ante not clear whether the market incorporates information conveyed by the disclosure that describes cyber risk.

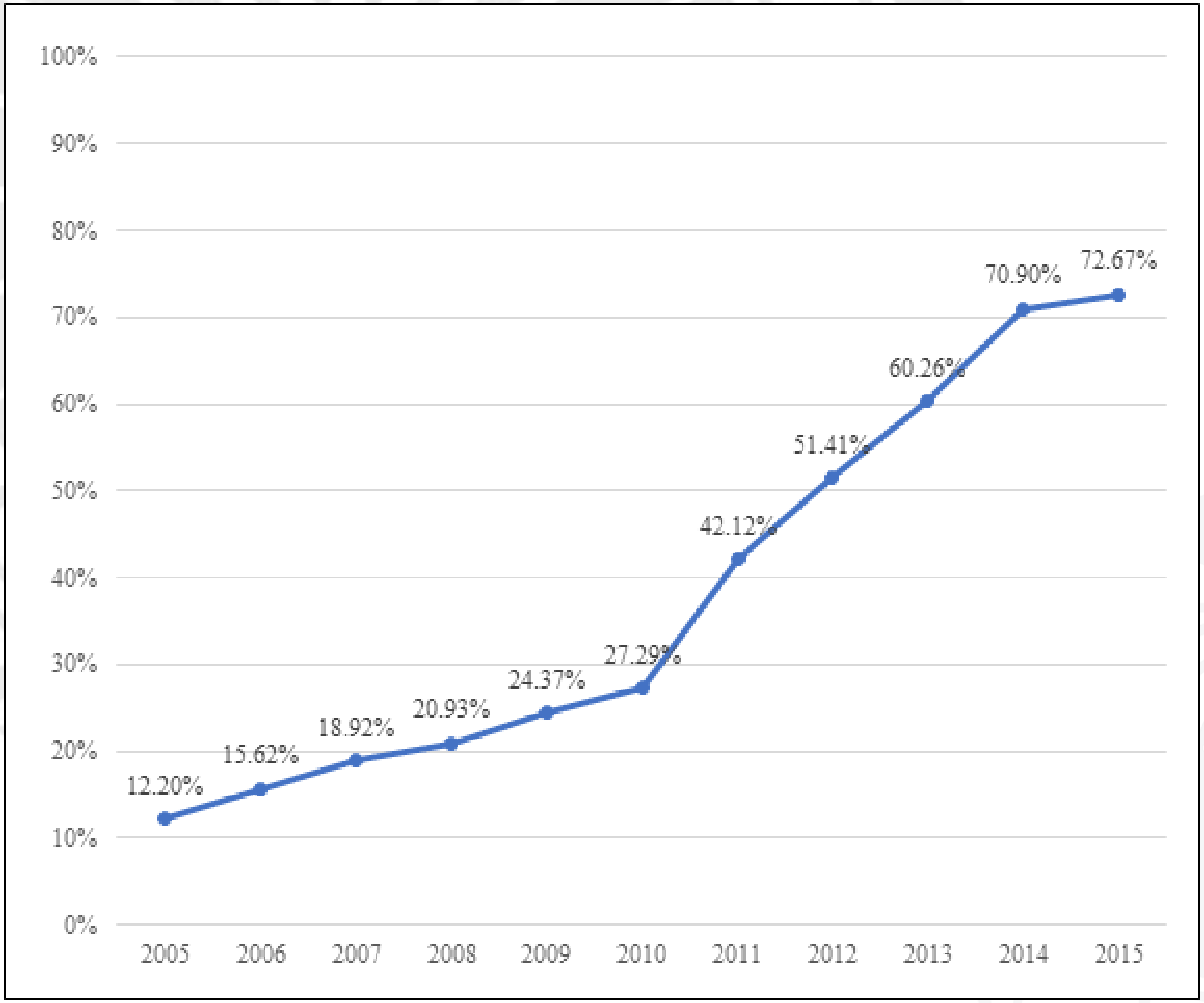
- If investors incorporate information from cybersecurity risk disclosure, they should respond less severely for firms with prior cybersecurity risk disclosure.

H3a. *The market reaction following cyber incident is less severe for firms with prior cyber risk disclosure.*

H3b. *The market reaction following cyber incident is less severe for firms with lengthy cyber risk disclosure.*



HYPOTHESIS



RUTGERS
Rutgers Business School
Newark and New Brunswick

HYPOTHESIS

- Since risk factor disclosure in item 1A is qualitative and does not require assessment of probability, firms may disclose all possible risk factors to fulfill regulatory requirement (Campbell et al., 2014).

- Consistent with this view, Beatty et al. (2015) document that disclosures become less reflective of future financial constraints following the SEC comment letters.

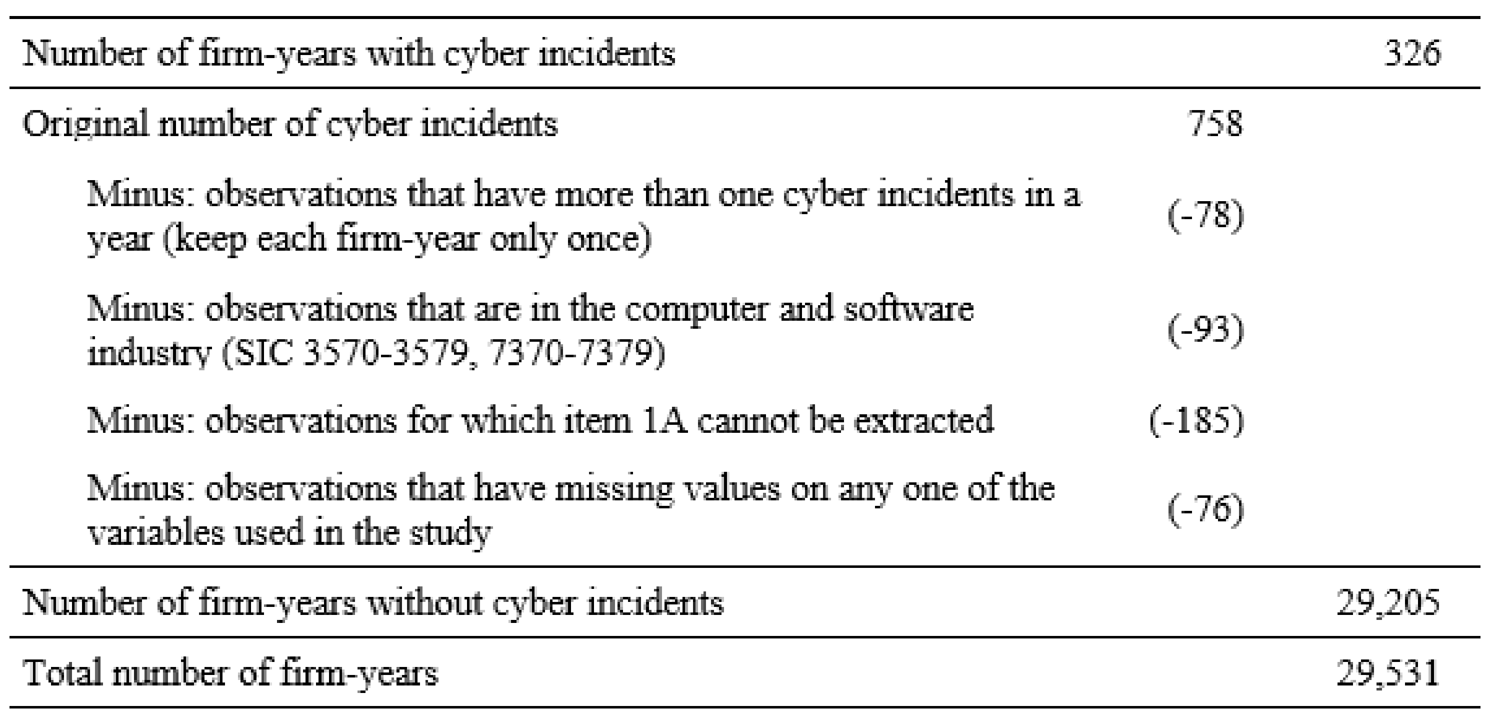
- To the extent that the SEC's cybersecurity disclosure guidance could be viewed as regulatory shock (i.e., regulatory pressure):

  H4. *The association between the presence of cyber risk disclosure and subsequent cyber incident is different before and after the introduction of the SEC's cybersecurity disclosure guidance.*

SAMPLE

- **Obtain cyber incident data from the Audit Analytics cybersecurity database and Privacy Rights Clearinghouse (privacyrights.org)**

- **Period between 2005 and 2015.**



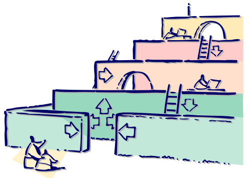
Number of firm-years with cyber incidents		326
Original number of cyber incidents	758	
Minus: observations that have more than one cyber incidents in a year (keep each firm-year only once)	(-78)	
Minus: observations that are in the computer and software industry (SIC 3570-3579, 7370-7379)	(-93)	
Minus: observations for which item 1A cannot be extracted	(-185)	
Minus: observations that have missing values on any one of the variables used in the study	(-76)	
Number of firm-years without cyber incidents		29,205
Total number of firm-years		29,531

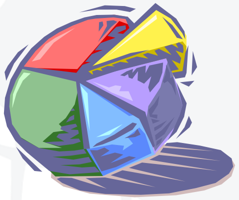
ESTIMATION MODEL

$$
\begin{aligned}
P(Breach_{it+1} = 1) = {} & Cyber\_Dislosure_{it} + Past\_Breach_{it} + Size_{it} + LN\_Segments_{it} \\
& + Age_{it} + Loss_{it} + LN\_Analyst_{it} + Foreign_{it} + Merger_{it} \\
& + Growth_{it} + ICW_{it} \qquad (1)
\end{aligned}
$$

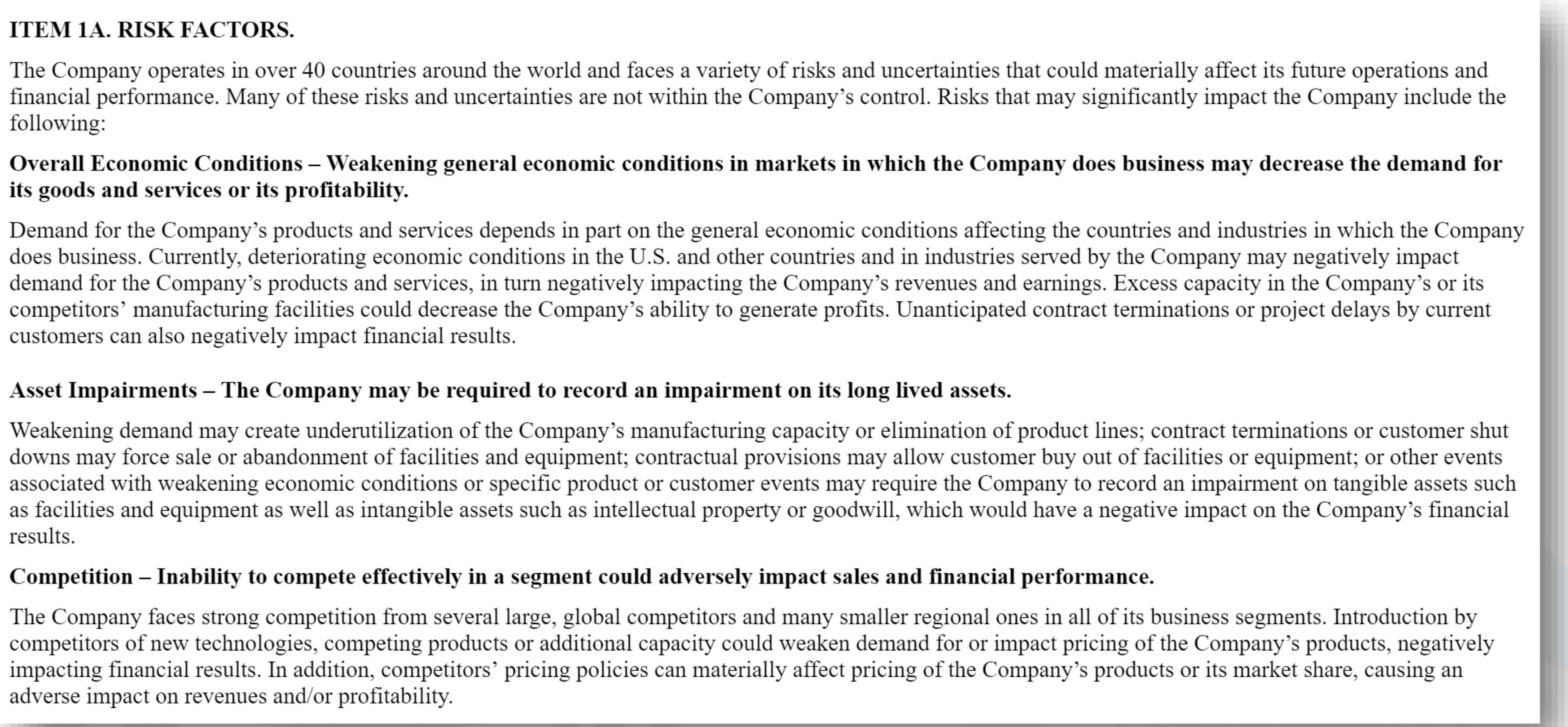
$$
\begin{aligned}
CAR_{it} = {} & Cyber\_Disclosure_{it} + Guidance_{it} + Market\_Cap_{it} + Severity_{it} \\
& + Leverage_{it} + Btm_{it} + Loss_{it} + \varepsilon_{it} \qquad (2)
\end{aligned}
$$

Disclosure	**Indicator variable, equal to 1 if the firm has cyber risk disclosure in fiscal year *t*, 0 otherwise**
Content	**Total number of words in cyber risk disclosure in fiscal year *t*, normalized by the average number of words in individual risk factors**





RISK FACTOR EXTRACTION



ITEM 1A. RISK FACTORS.

The Company operates in over 40 countries around the world and faces a variety of risks and uncertainties that could materially affect its future operations and financial performance. Many of these risks and uncertainties are not within the Company's control. Risks that may significantly impact the Company include the following:

Overall Economic Conditions – Weakening general economic conditions in markets in which the Company does business may decrease the demand for its goods and services or its profitability.

Demand for the Company's products and services depends in part on the general economic conditions affecting the countries and industries in which the Company does business. Currently, deteriorating economic conditions in the U.S. and other countries and in industries served by the Company may negatively impact demand for the Company's products and services, in turn negatively impacting the Company's revenues and earnings. Excess capacity in the Company's or its competitors' manufacturing facilities could decrease the Company's ability to generate profits. Unanticipated contract terminations or project delays by current customers can also negatively impact financial results.

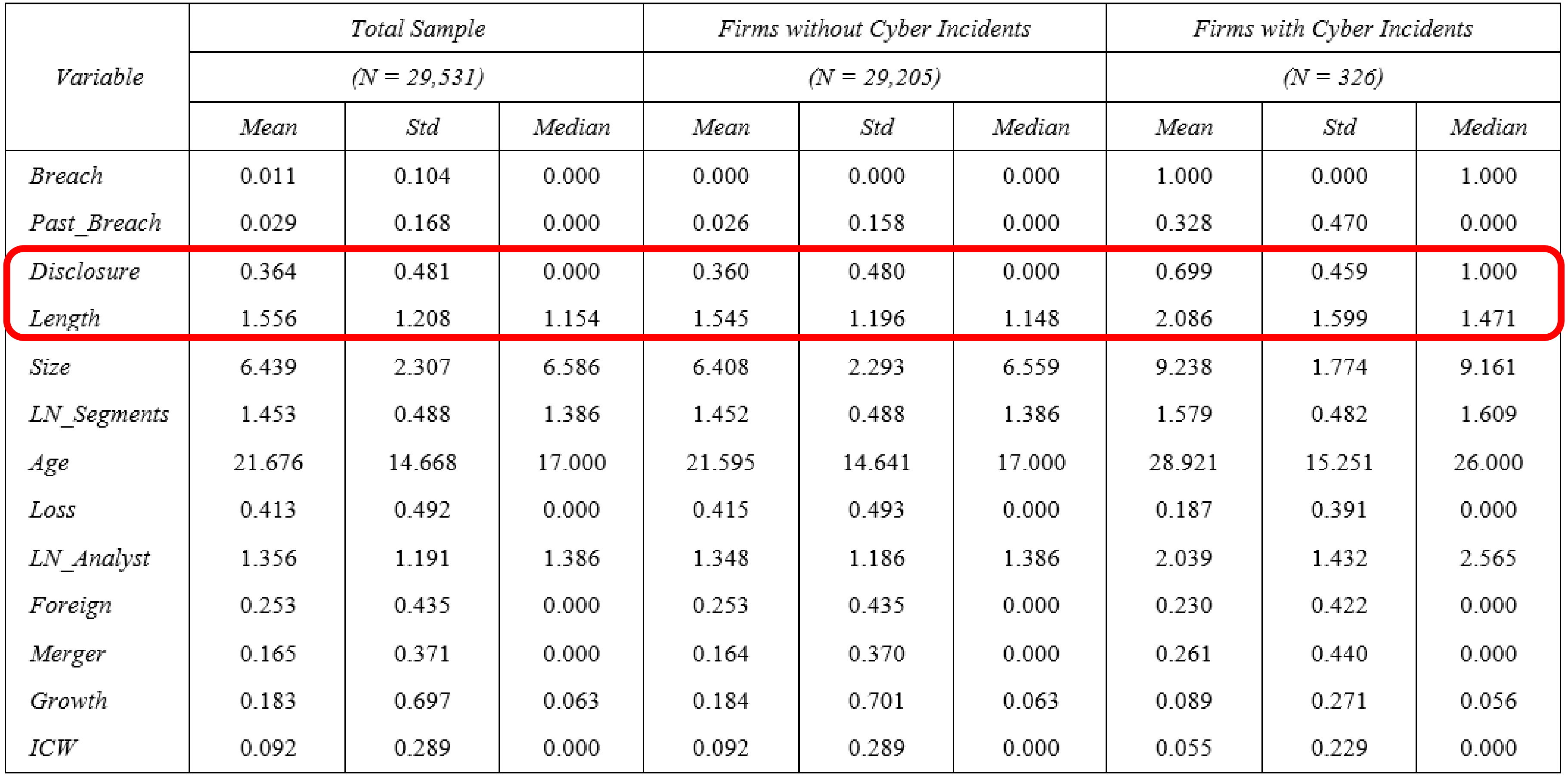
Asset Impairments – The Company may be required to record an impairment on its long lived assets.

Weakening demand may create underutilization of the Company's manufacturing capacity or elimination of product lines; contract terminations or customer shut downs may force sale or abandonment of facilities and equipment; contractual provisions may allow customer buy out of facilities or equipment; or other events associated with weakening economic conditions or specific product or customer events may require the Company to record an impairment on tangible assets such as facilities and equipment as well as intangible assets such as intellectual property or goodwill, which would have a negative impact on the Company's financial results.

Competition – Inability to compete effectively in a segment could adversely impact sales and financial performance.

The Company faces strong competition from several large, global competitors and many smaller regional ones in all of its business segments. Introduction by competitors of new technologies, competing products or additional capacity could weaken demand for or impact pricing of the Company's products, negatively impacting financial results. In addition, competitors' pricing policies can materially affect pricing of the Company's products or its market share, causing an adverse impact on revenues and/or profitability.

DESCRIPTIVE STATISTICS



Variable	*Total Sample*			*Firms without Cyber Incidents*			*Firms with Cyber Incidents*		
	(N = 29,531)			*(N = 29,205)*			*(N = 326)*		
	Mean	*Std*	*Median*	*Mean*	*Std*	*Median*	*Mean*	*Std*	*Median*
Breach	0.011	0.104	0.000	0.000	0.000	0.000	1.000	0.000	1.000
Past_Breach	0.029	0.168	0.000	0.026	0.158	0.000	0.328	0.470	0.000
Disclosure	0.364	0.481	0.000	0.360	0.480	0.000	0.699	0.459	1.000
Length	1.556	1.208	1.154	1.545	1.196	1.148	2.086	1.599	1.471
Size	6.439	2.307	6.586	6.408	2.293	6.559	9.238	1.774	9.161
LN_Segments	1.453	0.488	1.386	1.452	0.488	1.386	1.579	0.482	1.609
Age	21.676	14.668	17.000	21.595	14.641	17.000	28.921	15.251	26.000
Loss	0.413	0.492	0.000	0.415	0.493	0.000	0.187	0.391	0.000
LN_Analyst	1.356	1.191	1.386	1.348	1.186	1.386	2.039	1.432	2.565
Foreign	0.253	0.435	0.000	0.253	0.435	0.000	0.230	0.422	0.000
Merger	0.165	0.371	0.000	0.164	0.370	0.000	0.261	0.440	0.000
Growth	0.183	0.697	0.063	0.184	0.701	0.063	0.089	0.271	0.056
ICW	0.092	0.289	0.000	0.092	0.289	0.000	0.055	0.229	0.000

RUTGERS
Rutgers Business School
Newark and New Brunswick

RESULTS

TEST FOR H1 AND H2

$$
\begin{aligned}
P(Breach_{it+1} = 1) = {} & Cyber\_Dislosure_{it} + Past\_Breach_{it} + Size_{it} + LN\_Segments_{it} \\
& + Age_{it} + Loss_{it} + LN\_Analyst_{it} + Foreign_{it} + Merger_{it} \\
& + Growth_{it} + ICW_{it} \qquad (1)
\end{aligned}
$$

Independent variables	*Panel A*		*Panel B*	
	Estimates	*z-statistics*	*Estimates*	*z-statistics*
Disclosure	0.742	3.85***		
Length			0.199	4.13***
Past_Breach	1.414	7.45***	1.337	6.90***
Size	0.611	11.49***	0.525	9.19***
LN_Segments	0.053	0.34	0.185	0.90
Age	-0.003	-0.65	-0.004	-0.75
Loss	-0.108	-0.68	-0.006	-0.03
LN_Analyst	0.104	2.01**	0.072	1.16
Foreign	-0.033	-0.20	0.061	0.35
Merger	0.247	1.62*	0.097	0.58
Growth	-0.125	-0.70	-0.063	-0.38
ICW	0.500	1.75**	0.080	0.19
Finance	-0.133	-0.65	-0.116	-0.50
Consumer	1.298	6.75***	1.205	5.33***
Intercept	-10.291	-22.12***	-9.168	-15.54
Year Effects	Included		Included	
Pseudo R Square	0.253		0.218	
# Observations	29,531		10,480	

- **Disclosure**

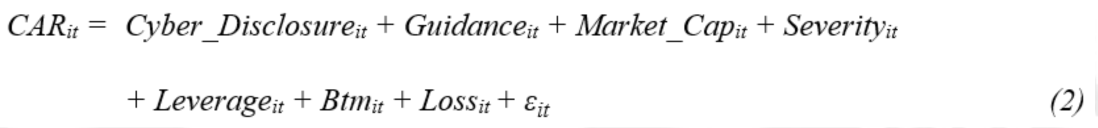
  Indicator variable, equal to 1 if the firm has cyber risk disclosure in fiscal year *t*, 0 otherwise

- **Content**

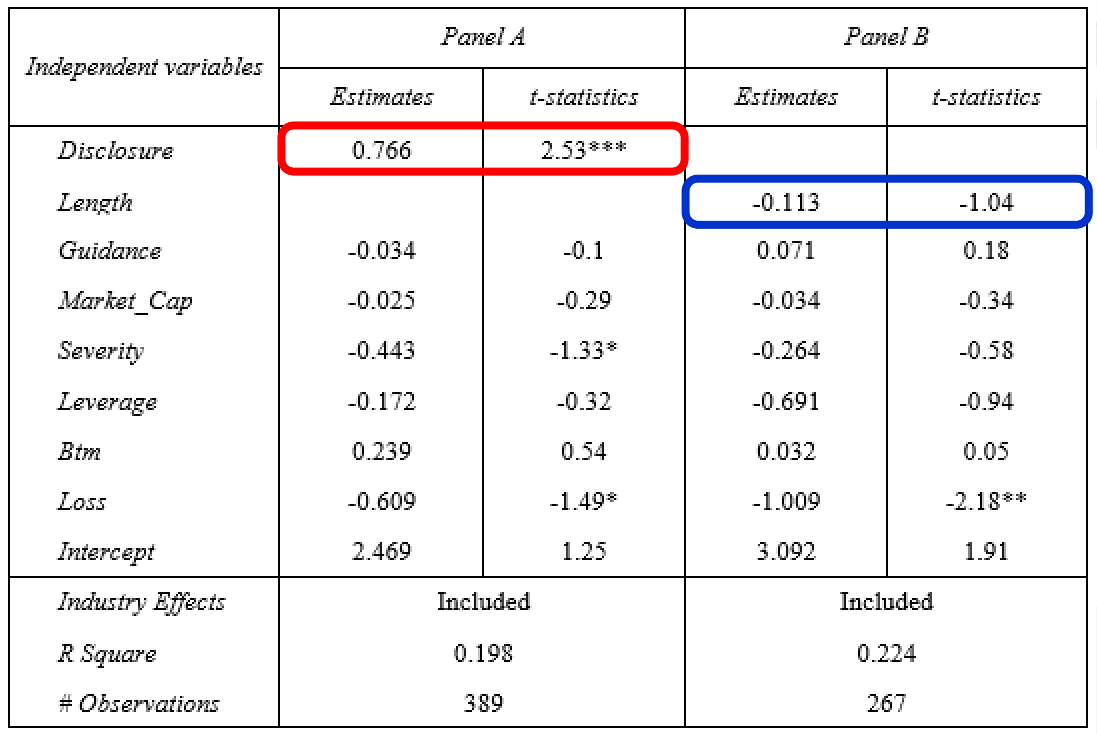
  Total number of words in cyber risk disclosure in fiscal year *t*, normalized by the average number of words in individual risk factors

RESULTS

TEST FOR H3a AND H3b



$$CAR_{it} = Cyber\_Disclosure_{it} + Guidance_{it} + Market\_Cap_{it} + Severity_{it} + Leverage_{it} + Btm_{it} + Loss_{it} + \varepsilon_{it} \qquad (2)$$



Independent variables	*Panel A*		*Panel B*	
	Estimates	*t-statistics*	*Estimates*	*t-statistics*
Disclosure	0.766	2.53***		
Length			-0.113	-1.04
Guidance	-0.034	-0.1	0.071	0.18
Market_Cap	-0.025	-0.29	-0.034	-0.34
Severity	-0.443	-1.33*	-0.264	-0.58
Leverage	-0.172	-0.32	-0.691	-0.94
Btm	0.239	0.54	0.032	0.05
Loss	-0.609	-1.49*	-1.009	-2.18**
Intercept	2.469	1.25	3.092	1.91
Industry Effects	Included		Included	
R Square	0.198		0.224	
# Observations	389		267	

- **Disclosure**

  Indicator variable, equal to 1 if the firm has cyber risk disclosure in fiscal year *t*, 0 otherwise

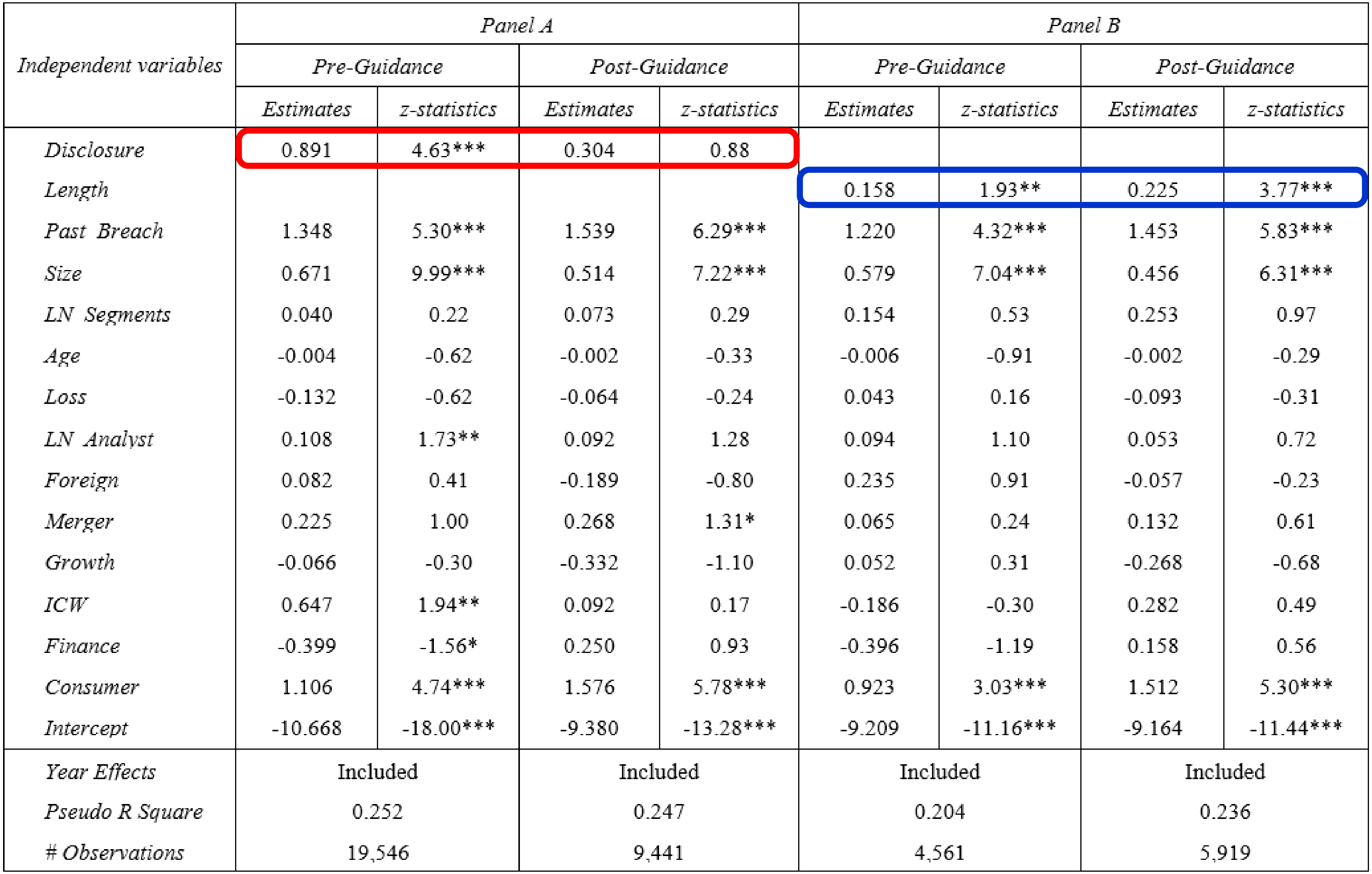
- **Content**

  Total number of words in cyber risk disclosure in fiscal year *t*, normalized by the average number of words in individual risk factors

Rutgers Business School
Newark and New Brunswick

RESULTS

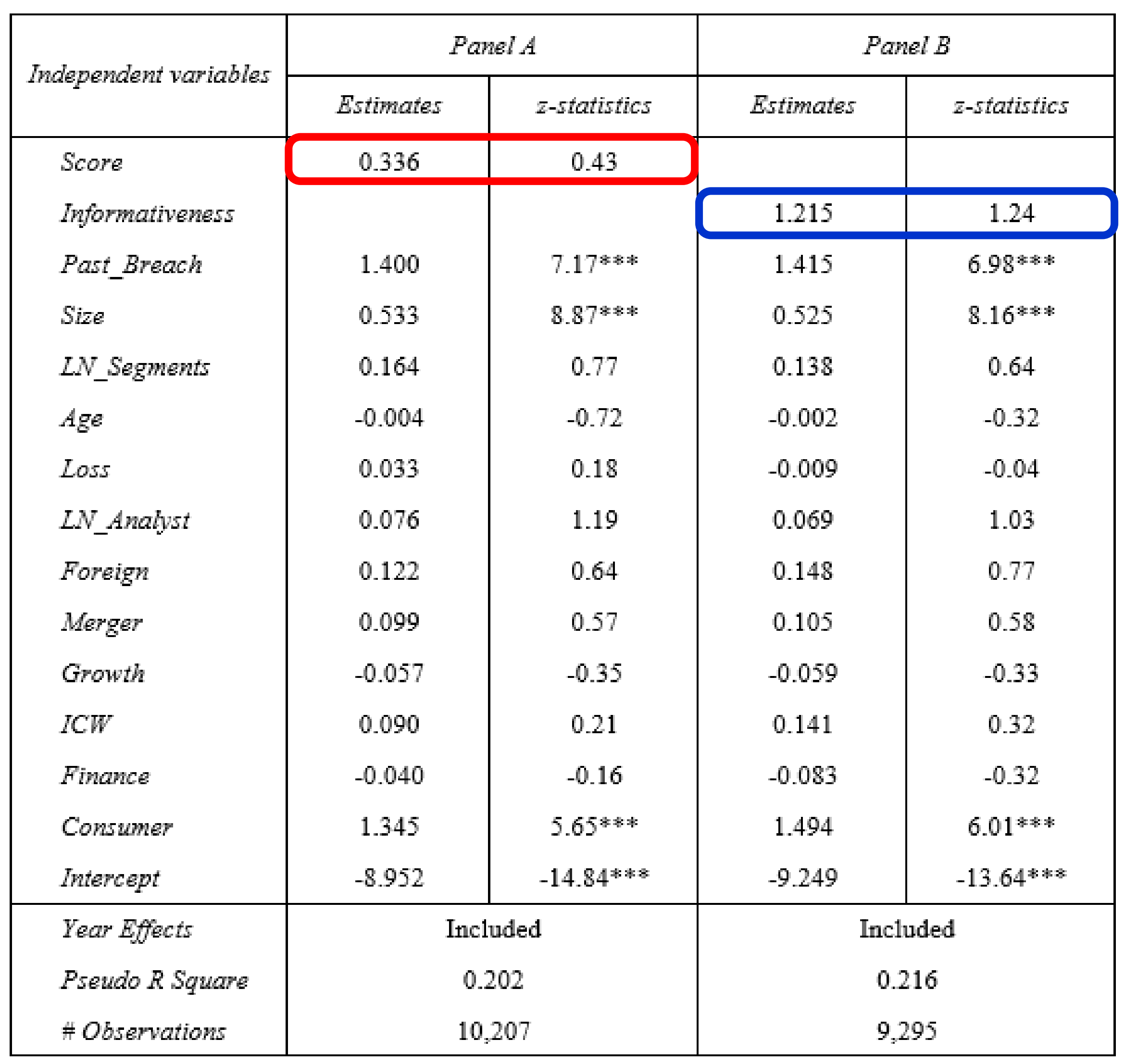
TEST FOR H4



Independent variables	*Panel A*				*Panel B*			
	Pre-Guidance		*Post-Guidance*		*Pre-Guidance*		*Post-Guidance*	
	Estimates	*z-statistics*	*Estimates*	*z-statistics*	*Estimates*	*z-statistics*	*Estimates*	*z-statistics*
Disclosure	0.891	4.63***	0.304	0.88				
Length					0.158	1.93**	0.225	3.77***
Past Breach	1.348	5.30***	1.539	6.29***	1.220	4.32***	1.453	5.83***
Size	0.671	9.99***	0.514	7.22***	0.579	7.04***	0.456	6.31***
LN Segments	0.040	0.22	0.073	0.29	0.154	0.53	0.253	0.97
Age	-0.004	-0.62	-0.002	-0.33	-0.006	-0.91	-0.002	-0.29
Loss	-0.132	-0.62	-0.064	-0.24	0.043	0.16	-0.093	-0.31
LN Analyst	0.108	1.73**	0.092	1.28	0.094	1.10	0.053	0.72
Foreign	0.082	0.41	-0.189	-0.80	0.235	0.91	-0.057	-0.23
Merger	0.225	1.00	0.268	1.31*	0.065	0.24	0.132	0.61
Growth	-0.066	-0.30	-0.332	-1.10	0.052	0.31	-0.268	-0.68
ICW	0.647	1.94**	0.092	0.17	-0.186	-0.30	0.282	0.49
Finance	-0.399	-1.56*	0.250	0.93	-0.396	-1.19	0.158	0.56
Consumer	1.106	4.74***	1.576	5.78***	0.923	3.03***	1.512	5.30***
Intercept	-10.668	-18.00***	-9.380	-13.28***	-9.209	-11.16***	-9.164	-11.44***
Year Effects	Included		Included		Included		Included	
Pseudo R Square	0.252		0.247		0.204		0.236	
# Observations	19,546		9,441		4,561		5,919	

ADDITIONAL TEST

FIRM-SPECIFC DISCLOSURES



Independent variables	*Panel A*		*Panel B*	
	Estimates	*z-statistics*	*Estimates*	*z-statistics*
Score	0.336	0.43		
Informativeness			1.215	1.24
Past_Breach	1.400	7.17***	1.415	6.98***
Size	0.533	8.87***	0.525	8.16***
LN_Segments	0.164	0.77	0.138	0.64
Age	-0.004	-0.72	-0.002	-0.32
Loss	0.033	0.18	-0.009	-0.04
LN_Analyst	0.076	1.19	0.069	1.03
Foreign	0.122	0.64	0.148	0.77
Merger	0.099	0.57	0.105	0.58
Growth	-0.057	-0.35	-0.059	-0.33
ICW	0.090	0.21	0.141	0.32
Finance	-0.040	-0.16	-0.083	-0.32
Consumer	1.345	5.65***	1.494	6.01***
Intercept	-8.952	-14.84***	-9.249	-13.64***
Year Effects	Included		Included	
Pseudo R Square	0.202		0.216	
# Observations	10,207		9,295	

- Investigate whether firm-specific cybersecurity risk disclosures are related with cyber incidents.
- Score

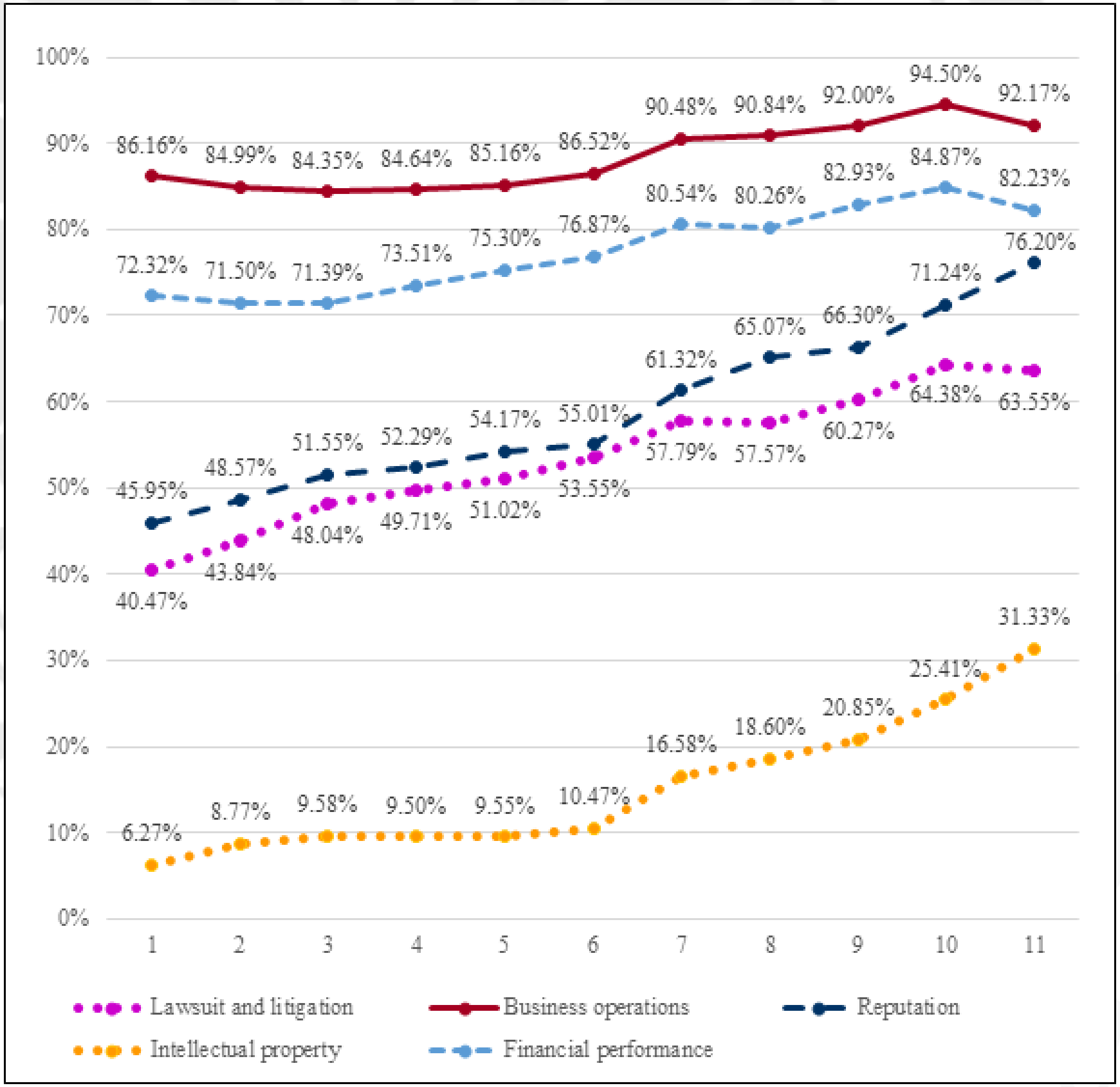
  One minus the cosine similarity score between firm's cyber risk disclosure and industry's average disclosure for fiscal year t, adjusted by length using Taylor expansion proposed by Brown and Tucker (2011)
- Informativeness

  Percentage of unique words that are not used by any other firms in the same industry for the same fiscal year

RUTGERS
Rutgers Business School
Newark and New Brunswick

ADDITIONAL ALAYSIS

TOPIC ANALYSIS



- Conduct a topic analysis to investigate firm’s concerns about cybersecurity.
- Extract two-word phrases that occur 2% - 98% (to remove specific phrases and uninformative phrases) of all cyber disclosures.
- Manually read and choose 211 meaningful phrases out of 1,042 phrases.
- Classify these phrases into five topics of consequences: business operations, financial performance, reputation, lawsuit and litigation, and intellectual property.

RUTGERS
Rutgers Business School
Newark and New Brunswick

CONCLUSION

- Both the presence and content of cyber risk disclosure are positively associated with subsequent cyber incidents, suggesting that cyber risk disclosure is not boilerplate.
- Investors are only using information conveyed by the presence of, but not the content of cyber risk disclosure.
- The presence of cyber risk disclosure is no longer associated with subsequent cyber incidents.
- Fail to find a significant association between firm-specific disclosure and cyber incidents.
- Firms are more concerned about the disruption of business operations and impact on financial performance when encountering cybersecurity issues. Moreover, there is a growing concern regarding reputational damage and loss of intellectual property due to cyber incidents.

LIMITATIONS

- Assume that managers have knowledge of the cybersecurity risks firms face, which may not necessarily hold. If firms are not aware of the level of cyber threats, they are less likely to provide meaningful disclosures.

- Use cyber incidents as the proxy for cybersecurity risks, which may not be the most accurate measure as theoretically any system can be breached.

- Did not answer the question why investors are not utilizing information conveyed in the content of cybersecurity risk disclosure.

COMMENTS & SUGGESTIONS

RUTGERS
Rutgers Business School
Newark and New Brunswick

CONTRIBUTIONS

- Contribute to the cybersecurity disclosure literature.
  - Complement Wang et al. (2013) and Gordon et al. (2010)
- Contribute to the risk disclosure literature.
  - Focus on actual risk event rather than perceived risk.
- Make contributions to the textual analysis literature.
  - Develop methods that first locate individual risk factors from item 1A and then identify security-related risk factors.
  - Topic analysis using word-term patterns help to obtain a thorough understanding with respect to the consequences of cyber incidents that firms are most concerned about.
- Help policy makers to determine the benefits and consequences of cyber risk disclosures and disclosure guidance.

LITERATURE REVIEW

- Campbell et al. (2014) show that firms disclose more risk factors when facing greater risks. The unexpected portion of risk factor disclosures is associated with systematic risk, idiosyncratic risk, information asymmetry, and abnormal returns following the disclosure.
- Kravet and Muslu (2013) reveal that increases in the number of risk-related sentences are positively associated with stock volatility, trading volume around and after the filings, and dispersed forecast revisions around the filings.
- Hope et al. (2016) demonstrate that the level of specificity in risk factor disclosures is positively associated with the market reaction and can help analysts assess firms' fundamental risk.
- Brown et al. (2015) identify that firms significantly modify their risk factor disclosures after receiving comment letters, and there exists spillover effect.
- Gaulin (2017) emphasizes the importance of using individual risk factors by showing that mangers add new risk factors and remove stale risk factors on a timely basis, and that such activities predict future economic changes even after controlling for ex ante risk and firm performance.

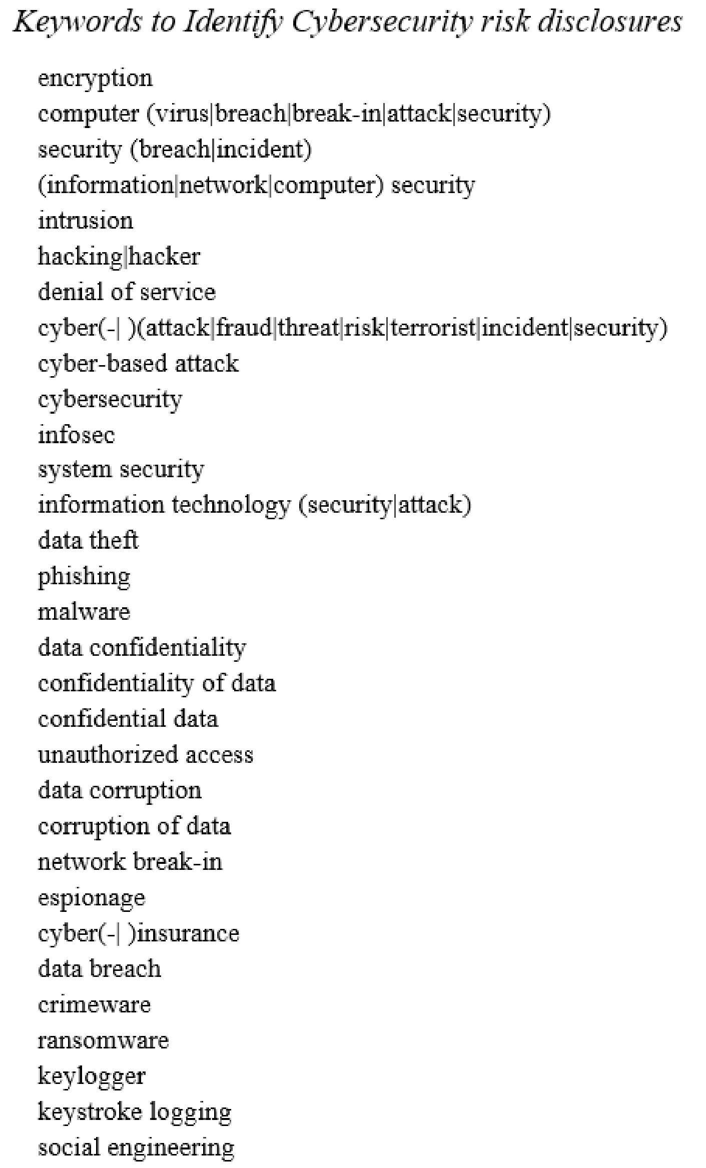
DATA SOURCE

- Audit Analytics Cybersecurity Database
  - Provide cybersecurity breaches for U.S. public firms
  - Updated once each quarter
  - Breaches are identified from three primary sources:
    - News agencies and Cybersecurity blogs
    - The Offices of the Attorney General of the following states: California, Maryland, New Hampshire, Vermont.
  - When available the following data is collected from the primary sources: Date of breach, Date became aware of breach, Disclosure date, Number of records stolen, Type of information stolen, Type of attack.
  - Once a breach is identified the following information from SEC 6-K/8-K filings is added as it is disclosed: The Disclosure, Costs, Insurance, Class actions.
- Privacy Rights Clearinghouse (privacyrights.org)
  - Publishes data breaches that involve individual's identity since 2005.
  - Include the following types of breaches: Payment Card Fraud, Hacking or Malware, Insider, Physical Loss, Portable Device, Stationary Device, Unintended Disclosure

VARIABLES

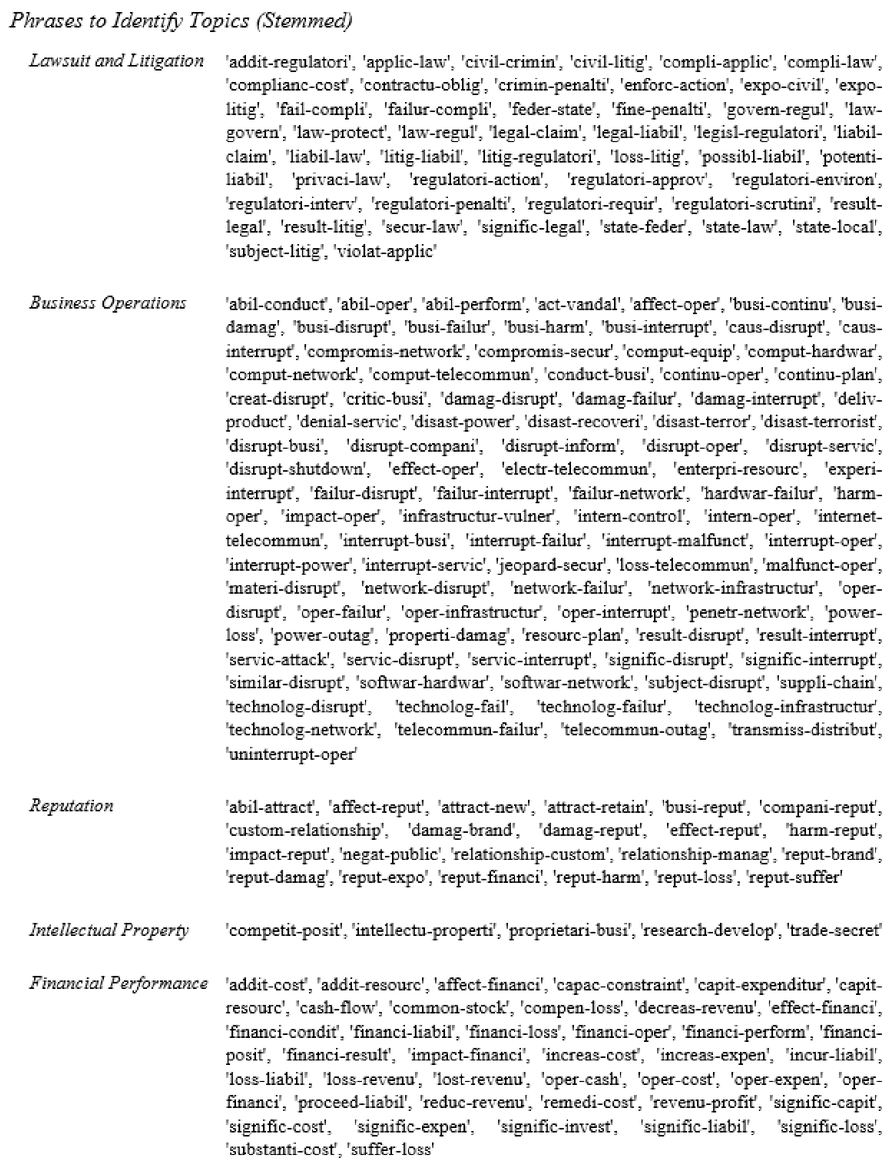
Variable	*Definition*
Breach	Indicator variable, equal to 1 if the firm experiences cyber incident(s) during fiscal year t, 0 otherwise;
Past Breach	Indicator variable, equal to 1 if the firm experiences cyber incident(s) in any year preceding fiscal year t, 0 otherwise;
Disclosure	Indicator variable, equal to 1 if the firm has cybersecurity risk disclosure in fiscal year t, 0 otherwise;
Length	Total number of words in cybersecurity risk disclosure in fiscal year t, normalized by the average number of words in individual risk factor disclosed in Item 1A;
Size	Natural log of total assets in millions in fiscal year t;
LN Segments	Natural log of number of business and geographic segments in fiscal year t;
Age	Number of year firms are included in CompuSmart in fiscal year t;
Loss	Indicator variable, equal to 1 if the firm reports negative net income in fiscal year t, 0 otherwise;
LN_Analyst	Natural log of number of analysts following in fiscal year t;
Foreign	Indicator variable, equal to 1 if the firm has foreign operations (based on FCA) in fiscal year t, 0 otherwise;
Merger	Indicator variable, equal to 1 if the firm is involved in merger activity in fiscal year t (based on AQP), 0 otherwise;
Growth	One-year growth rate in sales in fiscal year t;
ICW	Indicator variable, equal to 1 if the auditor reports an internal control weakness in fiscal year t, 0 otherwise;
Finance	Indicator variable, equal to 1 if the firm operates in finance industry (i.e. SIC between 6000 and 6999);
Consumer	Indicator variable, equal to 1 if the firm operates in consumer goods industry (i.e. SIC between 5200 and 5999);
Guidance	Indicator variable, equal to 1 after 2011, 0 otherwise;
Market Cap	Natural log of market capitalization of common stock in fiscal year t;
Severity	Indicator variable, equal to 1 if the cyber incident involves hacking by third parties, 0 otherwise;
Leverage	Total liabilities divided by total assets in fiscal year t;
Btm	Book value of common equity divided by market value of common equity in fiscal year t;
Score	One minus the cosine similarity score between firm's cybersecurity risk disclosure and industry's average disclosure for fiscal year t, adjusted by length using Taylor expansion proposed by Brown and Tucker (2011)
Informativeness	Percentage of unique words that are not used by any other firms in the same industry for the same fiscal year

KEYWORDS AND PHARASES



Keywords to Identify Cybersecurity risk disclosures

encryption
computer (virus|breach|break-in|attack|security)
security (breach|incident)
(information|network|computer) security
intrusion
hacking|hacker
denial of service
cyber(-|)(attack|fraud|threat|risk|terrorist|incident|security)
cyber-based attack
cybersecurity
infosec
system security
information technology (security|attack)
data theft
phishing
malware
data confidentiality
confidentiality of data
confidential data
unauthorized access
data corruption
corruption of data
network break-in
espionage
cyber(-|)insurance
data breach
crimeware
ransomware
keylogger
keystroke logging
social engineering



Phrases to Identify Topics (Stemmed)

Lawsuit and Litigation	'addit-regulatori', 'applic-law', 'civil-crimin', 'civil-litig', 'compli-applic', 'compli-law', 'complianc-cost', 'contractu-oblig', 'crimin-penalti', 'enforc-action', 'expo-civil', 'expo-litig', 'fail-compli', 'failur-compli', 'feder-state', 'fine-penalti', 'govern-regul', 'law-govern', 'law-protect', 'law-regul', 'legal-claim', 'legal-liabil', 'legisl-regulatori', 'liabil-claim', 'liabil-law', 'litig-liabil', 'litig-regulatori', 'loss-litig', 'possibl-liabil', 'potenti-liabil', 'privaci-law', 'regulatori-action', 'regulatori-approv', 'regulatori-environ', 'regulatori-interv', 'regulatori-penalti', 'regulatori-requir', 'regulatori-scrutini', 'result-legal', 'result-litig', 'secur-law', 'signific-legal', 'state-feder', 'state-law', 'state-local', 'subject-litig', 'violat-applic'
Business Operations	'abil-conduct', 'abil-oper', 'abil-perform', 'act-vandal', 'affect-oper', 'busi-continu', 'busi-damag', 'busi-disrupt', 'busi-failur', 'busi-harm', 'busi-interrupt', 'caus-disrupt', 'caus-interrupt', 'compromis-network', 'compromis-secur', 'comput-equip', 'comput-hardwar', 'comput-network', 'comput-telecommun', 'conduct-busi', 'continu-oper', 'continu-plan', 'creat-disrupt', 'critic-busi', 'damag-disrupt', 'damag-failur', 'damag-interrupt', 'deliv-product', 'denial-servic', 'disast-power', 'disast-recoveri', 'disast-terror', 'disast-terrorist', 'disrupt-busi', 'disrupt-compani', 'disrupt-inform', 'disrupt-oper', 'disrupt-servic', 'disrupt-shutdown', 'effect-oper', 'electr-telecommun', 'enterpri-resourc', 'experi-interrupt', 'failur-disrupt', 'failur-interrupt', 'failur-network', 'hardwar-failur', 'harm-oper', 'impact-oper', 'infrastructur-vulner', 'intern-control', 'intern-oper', 'internet-telecommun', 'interrupt-busi', 'interrupt-failur', 'interrupt-malfunct', 'interrupt-oper', 'interrupt-power', 'interrupt-servic', 'jeopard-secur', 'loss-telecommun', 'malfunct-oper', 'materi-disrupt', 'network-disrupt', 'network-failur', 'network-infrastructur', 'oper-disrupt', 'oper-failur', 'oper-infrastructur', 'oper-interrupt', 'penetr-network', 'power-loss', 'power-outag', 'properti-damag', 'resourc-plan', 'result-disrupt', 'result-interrupt', 'servic-attack', 'servic-disrupt', 'servic-interrupt', 'signific-disrupt', 'signific-interrupt', 'similar-disrupt', 'softwar-hardwar', 'softwar-network', 'subject-disrupt', 'suppli-chain', 'technolog-disrupt', 'technolog-fail', 'technolog-failur', 'technolog-infrastructur', 'technolog-network', 'telecommun-failur', 'telecommun-outag', 'transmiss-distribut', 'uninterrupt-oper'
Reputation	'abil-attract', 'affect-reput', 'attract-new', 'attract-retain', 'busi-reput', 'compani-reput', 'custom-relationship', 'damag-brand', 'damag-reput', 'effect-reput', 'harm-reput', 'impact-reput', 'negat-public', 'relationship-custom', 'relationship-manag', 'reput-brand', 'reput-damag', 'reput-expo', 'reput-financi', 'reput-harm', 'reput-loss', 'reput-suffer'
Intellectual Property	'competit-posit', 'intellectu-properti', 'proprietari-busi', 'research-develop', 'trade-secret'
Financial Performance	'addit-cost', 'addit-resourc', 'affect-financi', 'capac-constraint', 'capit-expenditur', 'capit-resourc', 'cash-flow', 'common-stock', 'compen-loss', 'decreas-revenu', 'effect-financi', 'financi-condit', 'financi-liabil', 'financi-loss', 'financi-oper', 'financi-perform', 'financi-posit', 'financi-result', 'impact-financi', 'increas-cost', 'increas-expen', 'incur-liabil', 'loss-liabil', 'loss-revenu', 'lost-revenu', 'oper-cash', 'oper-cost', 'oper-expen', 'oper-financi', 'proceed-liabil', 'reduc-revenu', 'remedi-cost', 'revenu-profit', 'signific-capit', 'signific-cost', 'signific-expen', 'signific-invest', 'signific-liabil', 'signific-loss', 'substanti-cost', 'suffer-loss'