Security in knowledge

INFOSEC INTELLIGENCE AND REGULATORY FILINGS

AN INVESTIGATION OF THE INFORMATION SECURITY CONTENT OF MANDATORY SEC DISCLOSURES

Chris Walsh

RSA CONFERENCE 2013

Session ID: SECT-35A

Session Classification: Intermediate

Motivation

- We all know incidents happen to everyone, sooner or later
- Some are more important than others. Some <u>really</u> matter.
- Where impact does matter, it's nice to inform those impacted.
  - State breach laws for consumers
  - SEC regulatory disclosures for investors and the public at large
- Gives stakeholders information upon which they can act

OUR FOCUS TODAY IS ON SEC REGULATORY DISCLOSURES AND THE INFO THEY CAN PROVIDE US IN INFORMATION SECURITY

New SEC guidance: October 13, 2011

Makes disclosure recommendations in several areas:

RISK FACTORS - “Registrants should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky.”

MD&A* - “Registrants should address cybersecurity risks and cyber incidents in their MD&A if the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant’s results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition.”

OTHER - Description of business, legal proceedings, financial statements, disclosure controls may be impacted

This updated guidance suggests an increased concern that information security risks have increased in potential severity or have been underreported to date.

* “Management discussion and analysis”

New SEC guidance: October 13, 2011

Makes disclosure recommendations in several areas:

RISK FACTORS - “Registrants should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky.”

MD&A* - “Registrants should address cybersecurity risks and cyber incidents in their MD&A if the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant’s results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition.”

OTHER - Description of business, legal proceedings, financial statements, disclosure controls may be impacted

This updated guidance suggests an increased concern that information security risks have increased in potential severity or have been underreported to date.

* “Management discussion and analysis”

“cyber” disclosures tend to be here

Table of Contents

EMC CORPORATION

		Page No.
	PART I	
ITEM 1.	Business	3
ITEM 1A.	Risk Factors	11
ITEM 1B.	Unresolved Staff Comments	20
ITEM 2.	Prope	
ITEM 3.	Legal	
ITEM 4.	Minc	
ITEM 5.	Mark	
ITEM 6.	Selec	
ITEM 7.	Mana	
ITEM 7A.	Quan	
ITEM 8.	Finan	
ITEM 9.	Chan	
ITEM 9A.	Contr	
ITEM 9B.	Other	
ITEM 10.	Direc	
ITEM 11.	Execu	
ITEM 12.	Secur	
ITEM 13.	Certa	
ITEM 14.	Princ	
ITEM 15.	Exhib	
Signatures		

ITEM 1A. RISK FACTORS

The risk factors that appear below could materially affect our business, financial condition and results of operations. The risks and uncertainties described below are not the only risks and uncertainties facing us. Our business is also subject to general risks and uncertainties that affect many other companies.

Our business could be materially adversely affected as a result of general economic and market conditions.

We are subject to the effects of general global economic and market conditions. If these conditions remain challenging or deteriorate, our business, results of operations or financial condition could be materially adversely affected. Possible consequences from uncertainty or further deterioration due to the recent global macroeconomic downturn on our business, including insolvency of key suppliers resulting in product delays, inability of customers to obtain credit to finance purchases of our products, customer insolvencies, increased risk that customers may delay payments, fail to pay or default on credit extended to them, and counterparty failures negatively impacting our treasury operations, could have a material adverse effect on our results of operations or financial condition.

[...]

Cybersecurity breaches could expose us to liability, damage our reputation, compromise our ability to conduct business, require us to incur significant costs or otherwise adversely affect our financial results.

We retain sensitive data, including intellectual property, proprietary business information and personally identifiable information, in our secure data centers and on our networks. We face a number of threats to our data centers and networks of unauthorized access, security breaches and other system disruptions. It is critical to our business strategy that our infrastructure remains secure and is perceived by customers and partners to be secure. Despite our security measures, our infrastructure may be vulnerable to attacks by hackers or other disruptive problems, such as the sophisticated cyber attack on our RSA division that we disclosed in March 2011. Any such security breach may compromise information stored on our networks and may result in significant data losses or theft of our, our customers’, our business partners’ or our employees’ intellectual property, proprietary business information or personally identifiable information. In addition, we have outsourced a number of our business functions to third party contractors, and any breach of their security systems could adversely affect us.

How can we assess broad impact?

In principle

- Look at all relevant filings, before and after.
- Perform textual analysis.
- Do filings differ?

How can we assess broad impact?

In principle

- Look at all relevant filings, before and after.
- Perform textual analysis.
- Do filings differ?

...but there are 30,000 filings

How can we assess broad impact?

In principle

- Look at all relevant filings, before and after.
- Perform textual analysis.
- Do filings differ?

...but there are 30,000 filings

We'll look at Fortune 500 subset

Data

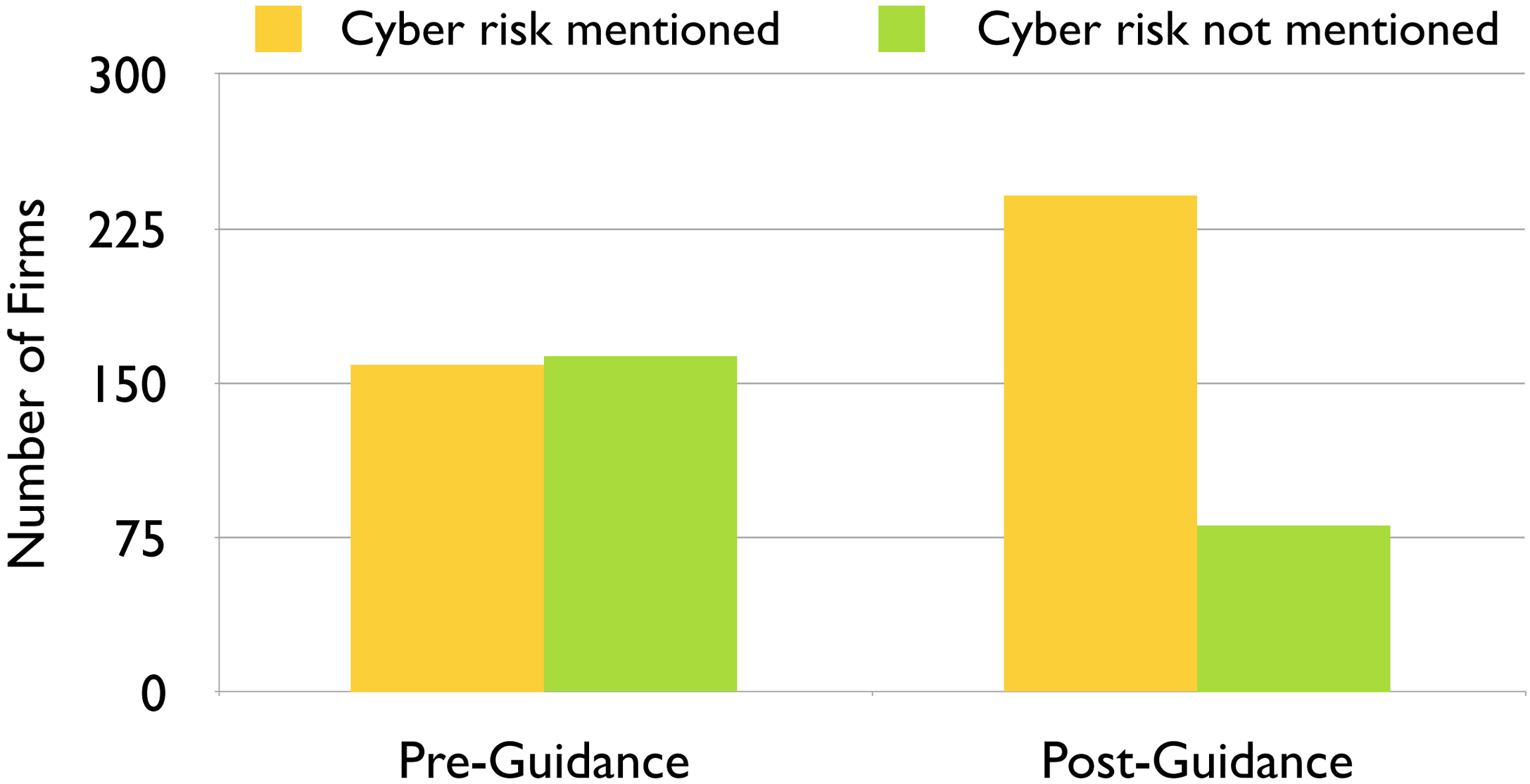
Fortune 500 firms of 2011, 2012

Those filing 10-Ks in 2011, 2012

Those with “Risk Factors” in both filings

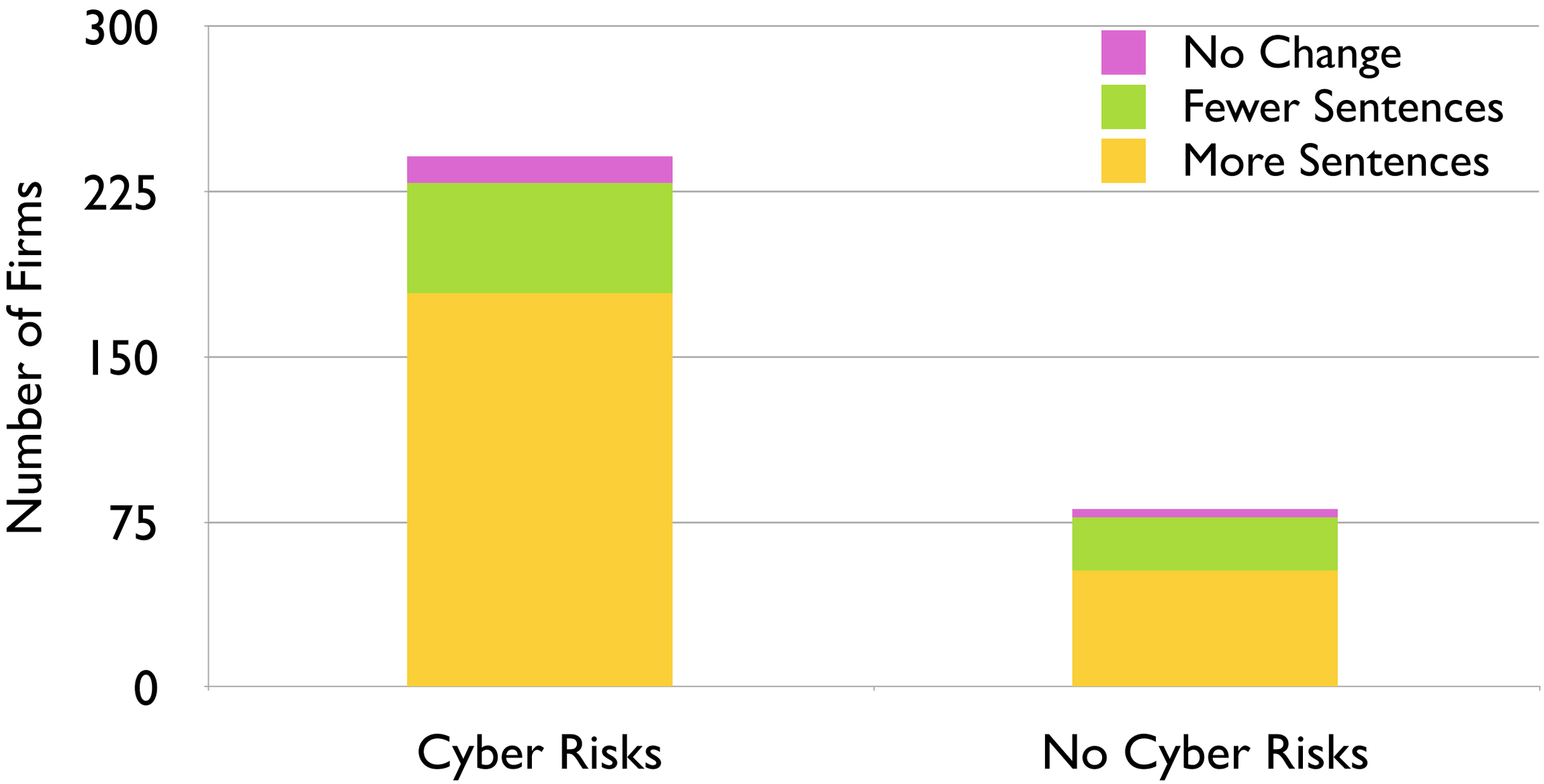
Resulting dataset has 322 firms, with reports before and after SEC revised guidance was issued

A Quick Graphical Summary



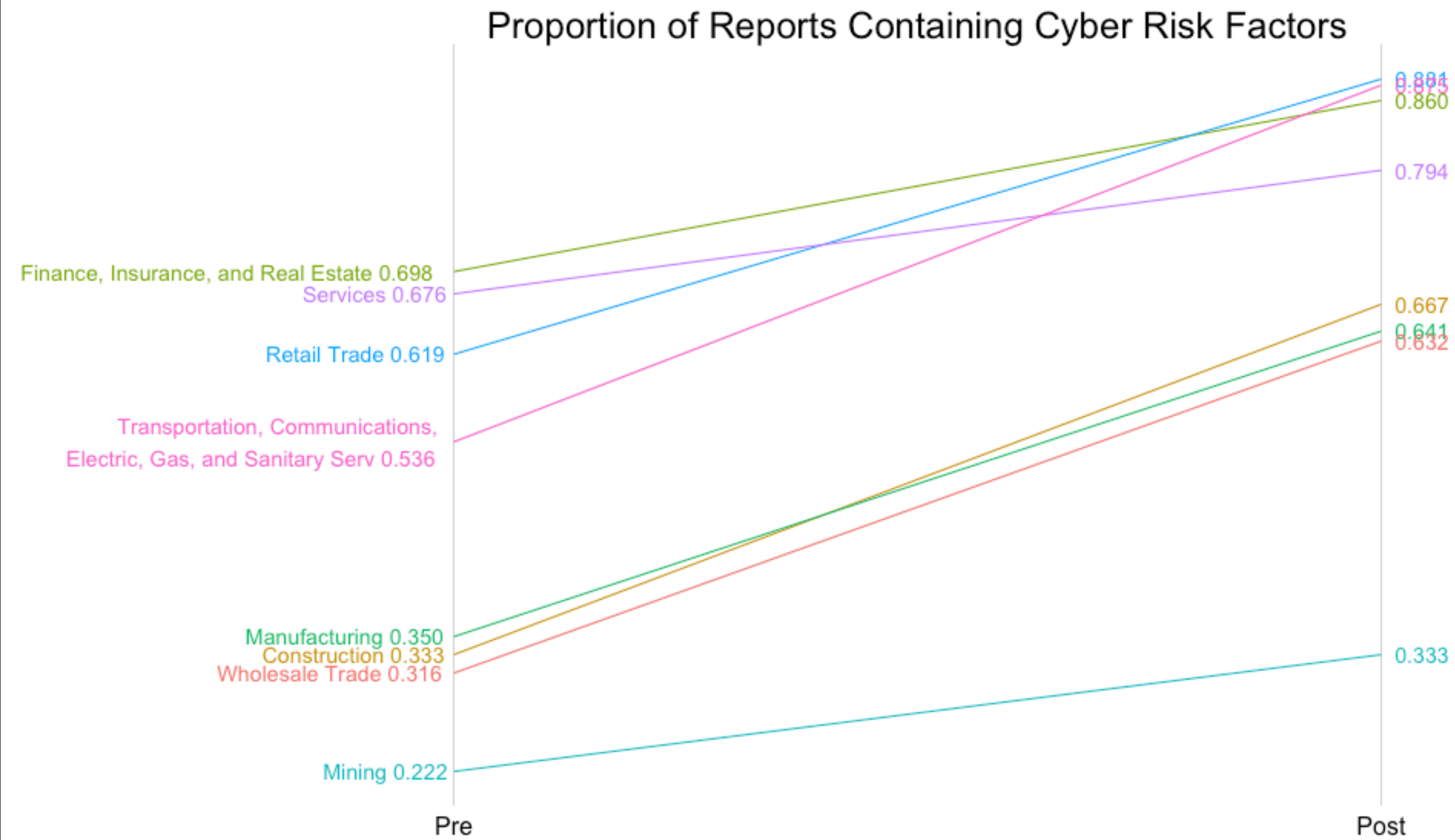
- Guidance seems to have made a difference!

Change in Risk Disclosure Size



Disclosures grew in general. "Cyber" more likely to have grown.

Reporting Change by Industry



Most frequent new word in 2012?

Most frequent new word in 2012?

“Cyber”

How many firms added which terms?

Word	Count		
cyber	97	reputation	34
attack	66	march	34
sovereign	62	intend	34
confidenti	62	cybersecur	33
european	54	critic	33
data	53	corrupt	33
unauthor	50	theft	32
europ	41	proprietari	32
breaches	41	measur	32
breach	39	august	32
information	37	viruses	31
comput	37		
network	36		
crisi	35		

15 of 25 terms added most often are ‘cyber’ related.

How many firms added which terms?

Word	Count		
cyber	97	reputation	34
attack	66	march	34
sovereign	62	intend	34
confidenti	62	cybersecur	33
european	54	critic	33
data	53	corrupt	33
unauthor	50	theft	32
europ	41	proprietari	32
breaches	41	measur	32
breach	39	august	32
information	37	viruses	31
comput	37		
network	36		
crisi	35		

15 of 25 terms added most often are ‘cyber’ related.

Arguably, 18 of 25 are.

What is/is not in these disclosures?

Three chosen at random: these show the typical case

One chosen deliberately: this shows an emerging trend

Legend:

Green: the threats

Red: the threat actors

Blue: what is threatened

Purple: possible consequences

Orange: Have attempts occurred?

Magenta: Were they successful?

Example – General Dynamics

"**Our business could be negatively impacted by cyber security events and other disruptions.** As a defense contractor, we face various cyber security threats, including threats to our information technology infrastructure and attempts to gain access to our proprietary or classified information, as well as threats to physical security. We also design and manage information technology systems for various customers. We generally face the same security threats for these systems as for our own. Accordingly, we maintain information security policies and procedures for managing all systems. If any of these threats materialize, the event could cause serious harm to our business, damage our reputation and prevent us from being eligible for future work on sensitive or classified systems for U.S. government customers and could have an adverse effect on our results of operations."

http://www.sec.gov/Archives/edgar/data/40533/000119312512066385/d271667d10k.htm

Example – General Dynamics

"**Our business could be negatively impacted by cyber security events and other disruptions.** As a defense contractor, we face various cyber security threats, including threats to our information technology infrastructure and attempts to gain access to our proprietary or classified information, as well as threats to physical security. We also design and manage information technology systems for various customers. We generally face the same security threats for these systems as for our own. Accordingly, we maintain information security policies and procedures for managing all systems. If any of these threats materialize, the event could cause serious harm to our business, damage our reputation and prevent us from being eligible for future work on sensitive or classified systems for U.S. government customers and could have an adverse effect on our results of operations."

Example – General Dynamics

"**Our business could be negatively impacted by cyber security events and other disruptions.** As a defense contractor, we face various cyber security threats, including threats to our information technology infrastructure and attempts to gain access to our proprietary or classified information, as well as threats to physical security. We also design and manage information technology systems for various customers. We generally face the same security threats for these systems as for our own. Accordingly, we maintain information security policies and procedures for managing all systems. If any of these threats materialize, the event could cause serious harm to our business, damage our reputation and prevent us from being eligible for future work on sensitive or classified systems for U.S. government customers and could have an adverse effect on our results of operations."

Example – Deere & Co.

Security breaches and other disruptions to the Company's information technology infrastructure could interfere with the Company's operations, and could compromise the Company's and its customers' and suppliers' information, exposing the Company to liability which would cause the Company's business and reputation to suffer.

In the ordinary course of business, the Company relies upon information technology networks and systems, some of which are managed by third parties, to process, transmit and store electronic information, and to manage or support a variety of business processes and activities, including supply chain, manufacturing, distribution, invoicing, and collection of payments from dealers or other purchasers of John Deere equipment and from customers of the Company's financial services operations. The Company uses information technology systems to record, process and summarize financial information and results of operations for internal reporting purposes and to comply with regulatory financial reporting, legal and tax requirements. Additionally, the Company collects and stores sensitive data, including intellectual property, proprietary business information, the propriety business information of our customers and suppliers, as well as personally identifiable information of the Company's customers and employees, in data centers and on information technology networks. The secure operation of these information technology networks, and the processing and maintenance of this information is critical to the Company's business operations and strategy. Despite security measures and business continuity plans, the Company's information technology networks and infrastructure may be vulnerable to damage, disruptions or shutdowns due to attacks by hackers or breaches due to employee error or malfeasance, or other disruptions during the process of upgrading or replacing computer software or hardware, power outages, computer viruses, telecommunication or utility failures or natural disasters or other catastrophic events. The occurrence of any of these events could compromise the Company's networks and the information stored there could be accessed, publicly disclosed, lost or stolen. Any such access, disclosure or other loss of information could result in legal claims or proceedings, liability or regulatory penalties under laws protecting the privacy of personal information, disrupt operations, and damage the Company's reputation, which could adversely affect the Company's business.

http://www.sec.gov/Archives/edgar/data/27673/000110465912084562/a12-24291_110k.htm

Example – Waste Management, Inc.

A cybersecurity incident could negatively impact our business and our relationships with customers.
We use computers in substantially all aspects of our business operations. We also use mobile devices, social networking and other online activities to connect with our employees and our customers. Such uses give rise to cybersecurity risks, including security breach, espionage, system disruption, theft and inadvertent release of information. Our business involves the storage and transmission of numerous classes of sensitive and/or confidential information and intellectual property, including customers' personal information, private information about employees, and financial and strategic information about the Company and its business partners. We also rely on a Payment Card Industry compliant third party to protect our customers' credit card information. Further, as the Company pursues its strategy to grow through acquisitions and to pursue new initiatives that improve our operations and cost structure, the Company is also expanding and improving its information technologies, resulting in a larger technological presence and corresponding exposure to cybersecurity risk. If we fail to assess and identify cybersecurity risks associated with acquisitions and new initiatives, we may become increasingly vulnerable to such risks. Additionally, while we have implemented measures to prevent security breaches and cyber incidents, our preventative measures and incident response efforts may not be entirely effective. The theft, destruction, loss, misappropriation, or release of sensitive and/or confidential information or intellectual property, or interference with our information technology systems or the technology systems of third parties on which we rely, could result in business disruption, negative publicity, brand damage, violation of privacy laws, loss of customers, potential liability and competitive disadvantage.

http://www.sec.gov/Archives/edgar/data/823768/000119312512065370/d260235d10k.htm

Example – Intel 2011

We may be subject to intellectual property theft or misuse, which could result in third-party claims and harm our business and results of operations.

We regularly face attempts by others to gain unauthorized access through the Internet to our information technology systems, such as when they masquerade as authorized users or surreptitiously introduce software. These attempts, which might be the result of industrial or other espionage, or actions by hackers seeking to harm the company, its products, or end users, are sometimes successful. We seek to detect and investigate these security incidents and to prevent their recurrence, but in some cases we might be unaware of an incident or its magnitude and effects.

http://www.sec.gov/Archives/edgar/data/50863/000095012311015783/f56033e10vk.htm

Example – Intel 2012

***Third parties** may attempt to **breach our network security**, which could **damage our reputation and financial results**.*

We regularly face attempts by others to gain unauthorized access through the Internet or introduce malicious software to our IT systems. These attempts—which might be the result of industrial or other espionage, or actions by hackers seeking to harm the company, its products, or end users—are sometimes successful. In part because of the high profile of our McAfee subsidiary in the network and system protection business, we might become a target of computer hackers who create viruses to sabotage or otherwise attack our products and services. Hackers might attempt to penetrate our network security and gain access to our network and our data centers, steal proprietary information, including personally identifiable information, or interrupt our internal systems and services. We seek to detect and investigate these security incidents and to prevent their recurrence, but in some cases we might be unaware of an incident or its magnitude and effects.

http://www.sec.gov/Archives/edgar/data/50863/000119312512075534/d302695d10k.htm

SEC reviews filings, leading to change

"[The Corporate Finance Division] selectively reviews filings of new issuers and public companies...to both monitor and enhance compliance with disclosure and accounting requirements.

[...]

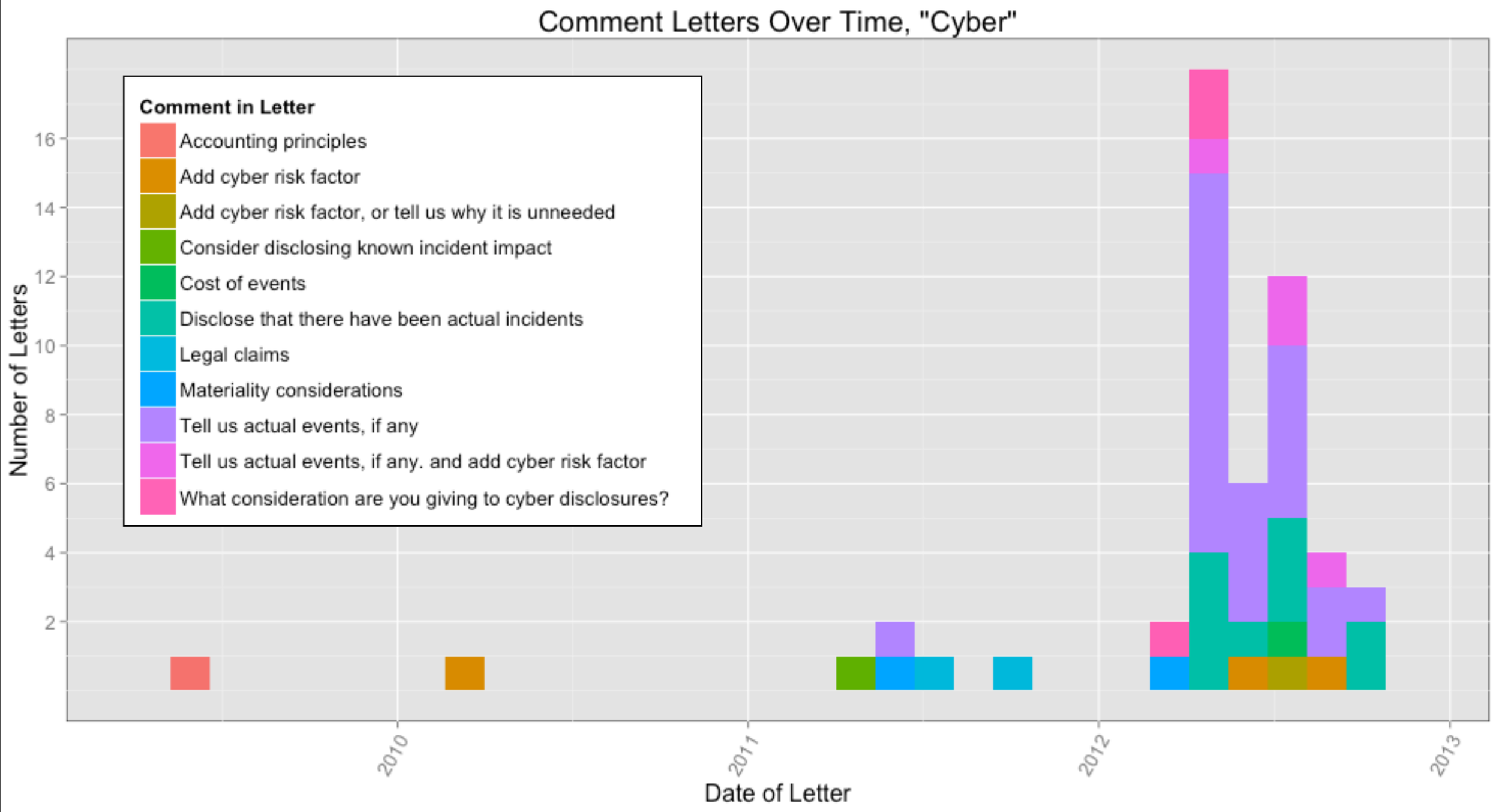
The staff members engaged in filing reviews have accounting and disclosure expertise aligned with the industries in their respective review groups. ***Approximately 80 percent of the staff of the Division is assigned to the disclosure review program***

[....]

In the course of a review, the staff will issue comments to a company to elicit better compliance with applicable disclosure requirements. In response to those comments, a company may need to amend its financial statements or other disclosures to provide additional or enhanced information, or may undertake to improve its disclosures in future filings."

http://www.sec.gov/news/testimony/2011/ts1116rk.htm

SEC “Comment Letters” as catalyst



Examples showing this future direction

SEC to Southwest Airlines, April 2, 2012

Risk Factors, page 23
Any failure of the Company to maintain the security, page 27

3. We note that you derive a significant percentage of revenues from internet bookings and rely on third party technology and systems for many of your technology initiatives. We also note that you disclose that customer information is subject to the risk of intrusion, tampering, and theft and that system disruptions could occur. Please tell us whether you have experienced attacks, disruptions, intrusions, tampering or theft in the past and, if so, whether disclosure of that fact would provide the proper context for your risk factor disclosures. Please refer to the Division of Corporation Finance's Disclosure Guidance Topic No. 2 at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm for additional information.

http://www.sec.gov/Archives/edgar/data/92380/000000000012016774/filename1.pdf

Future direction – cont'd

Southwest Airlines response, April 16, 2012

The Company has not experienced cyber incidents that are individually, or in the aggregate, material. In addition, **the Company is sensitive to the Commission's guidance that it should not present risks that could apply to any issuer**. Nevertheless, the Company recognizes that cyber risks and vulnerabilities continue to evolve and that developing and maintaining adequate security measures may present significant challenges not only for the Company, but also for third parties with which the Company does business. Therefore, the Company's risk factor provides examples of (i) the significant *types* of cybersecurity risks that the Company monitors and seeks to address on an ongoing basis, (ii) the aspects of the Company's operations that give rise to such risks, and (iii) potential consequences to the Company should it not be able to adequately address these risks. In accordance with the Division of Corporation Finance's Disclosure Guidance Topic No. 2, **the Company does not believe additional detail is necessary to provide the proper context for the risk factor**

http://www.sec.gov/Archives/edgar/data/92380/000009238012000012/filename1.htm

Future direction – cont'd

SEC, April 27, 2012

In response to prior comment 3, you disclose that you recognize that cyber risks and vulnerabilities continue to evolve and that developing and maintaining adequate security measures may present significant challenges not only for you, but also for third parties with which you do business. Accordingly, **it appears that your business has been subject to cyber risks. If you have experienced attacks in the past, please expand your risk factor to state that.**

http://www.sec.gov/Archives/edgar/data/92380/000000000012021869/filename1.pdf

Southwest, April 27, 2012

Although the Company has not experienced cyber incidents that are individually, or in the aggregate, material, **the Company will comply with the Staff's request and will expand its risk factor disclosure in future filings to state that it has experienced cyber attacks in the past, which have thus far been mitigated by preventive and detective measures put in place by the Company**.

http://www.sec.gov/Archives/edgar/data/92380/000009238012000022/filename1.htm

Example 2: Wal-Mart

SEC, June 8, 2012

We note your disclosure that you "may be vulnerable to security breaches" through cyber attacks. **Please tell us whether any such breaches or attacks have occurred in the past. In order to place the risks described in this risk factor in an appropriate context, in future filings please expand your risk factor to disclose this information.**

http://www.sec.gov/Archives/edgar/data/104169/000000000012029999/filename1.pdf

Wal-Mart, June 22, 2012

[...] in the future the Company will modify its risk factor disclosure relating to the risk discussed in the Subject Risk Factor to read substantially as follows: [...]

Each year, computer hackers make numerous attempts to access the information stored in our information systems. We maintain substantial security measures to protect, and to prevent unauthorized access to, such information. As a result of those measures, the **past attempts by computer hackers to gain access to the information stored on our information systems have been unsuccessful.**

http://www.sec.gov/Archives/edgar/data/104169/000144530512002043/filename1.htm

What will future disclosures look like?

- More firms from all industries mentioning cyber risks
- More firms disclosing that they have actually been subject to these threats
- More firms acknowledging that sometimes attacks have worked

Implications

Disclosure of immaterial incidents

- Need to track and speak of small incidents in boardroom-ready terms
- Need to understand concept of materiality
  - Why an incident matters, and to whom

Need to see where your industry is

SEC's requests to your peers likely pertain to you as well

Last, but not least

“Stuff happens”

Increased disclosure, and events outside the disclosure realm, show more firms are acknowledging incidents.

More information -> better decisions, less fear/shame.

Acknowledgments

My interest in this topic was inspired by

- Various blog postings made by Adam Shostack and Richard Bejtlich
- Discussion on the Security Metrics mailing list
- The example set by the OSF's Primary Sources Archive, and by
- The recent reporting of Joseph Menn and Linda Sandler.

Questions?