MIRcon 2012

Reading the SEC's mail

Trends in "cyber" incidents and risk, as revealed through public correspondence with regulated firms

Chris Walsh

chris@cwalsh.org

Disclaimer

I am not a lawyer or an accountant.

Use of “cyber-” does not imply endorsement, but as with “hacker”, it reflects a grudging recognition of common usage.

Opinions are mine as an individual.

I may speak quickly.

Talk outline

- Brief overview of SEC's role as a regulator
- Description of specific forms and sections of forms relevant to Infosec
- Overview of the primary source repository used: "the SEC's mail"
- Basic quantitative snapshot, including variations over time
- Drill-down into three time periods
  - Well before October 13, 2011 revised guidance
  - Just before October 13, 2011 revised guidance
  - After October 13, 2011 revised guidance
- Closing observations
- Questions

The role of the SEC

"The mission of the U.S. Securities and Exchange Commission is to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation.

[...]

The laws and rules that govern the securities industry in the United States derive from a simple and straightforward concept: all investors, whether large institutions or private individuals, should have access to certain basic facts about an investment prior to buying it, and so long as they hold it. To achieve this, the SEC requires public companies to disclose meaningful financial and other information to the public."

http://www.sec.gov/about/whatwedo.shtml

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”

The SEC doesn't just passively receive forms

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

[...]

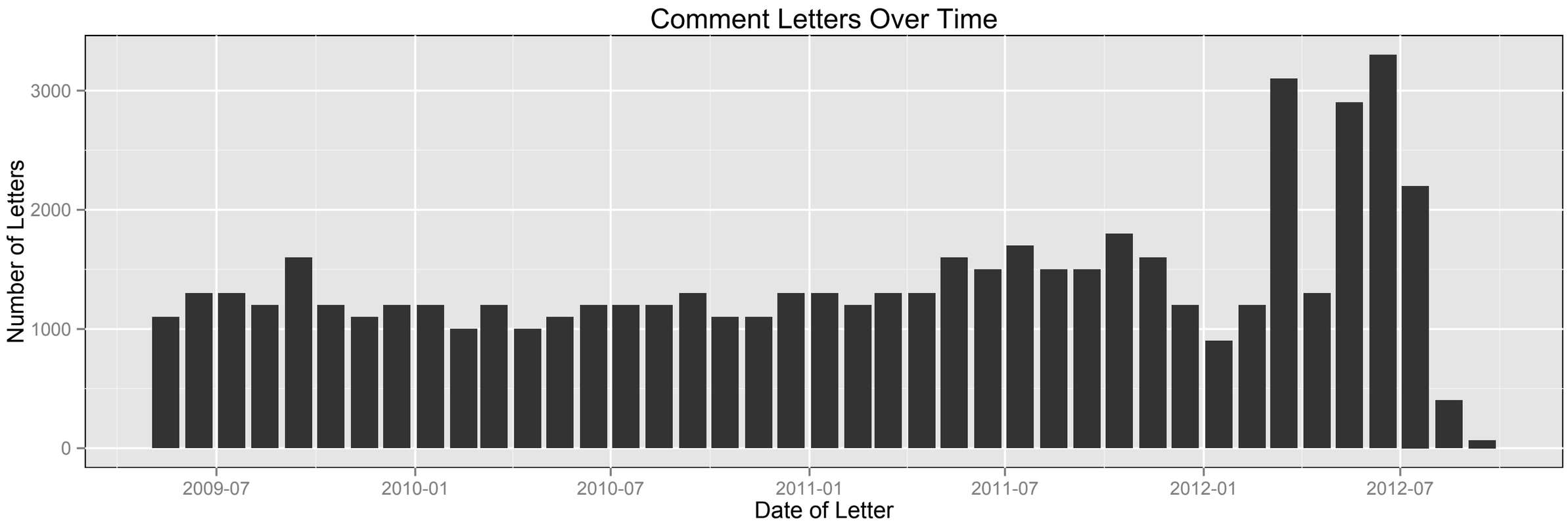
The staff members engaged in filing reviews have accounting and disclosure expertise aligned with the industries in their respective review groups. *Approximately 80 percent of the staff of the Division is assigned to the disclosure review program*

[....]

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

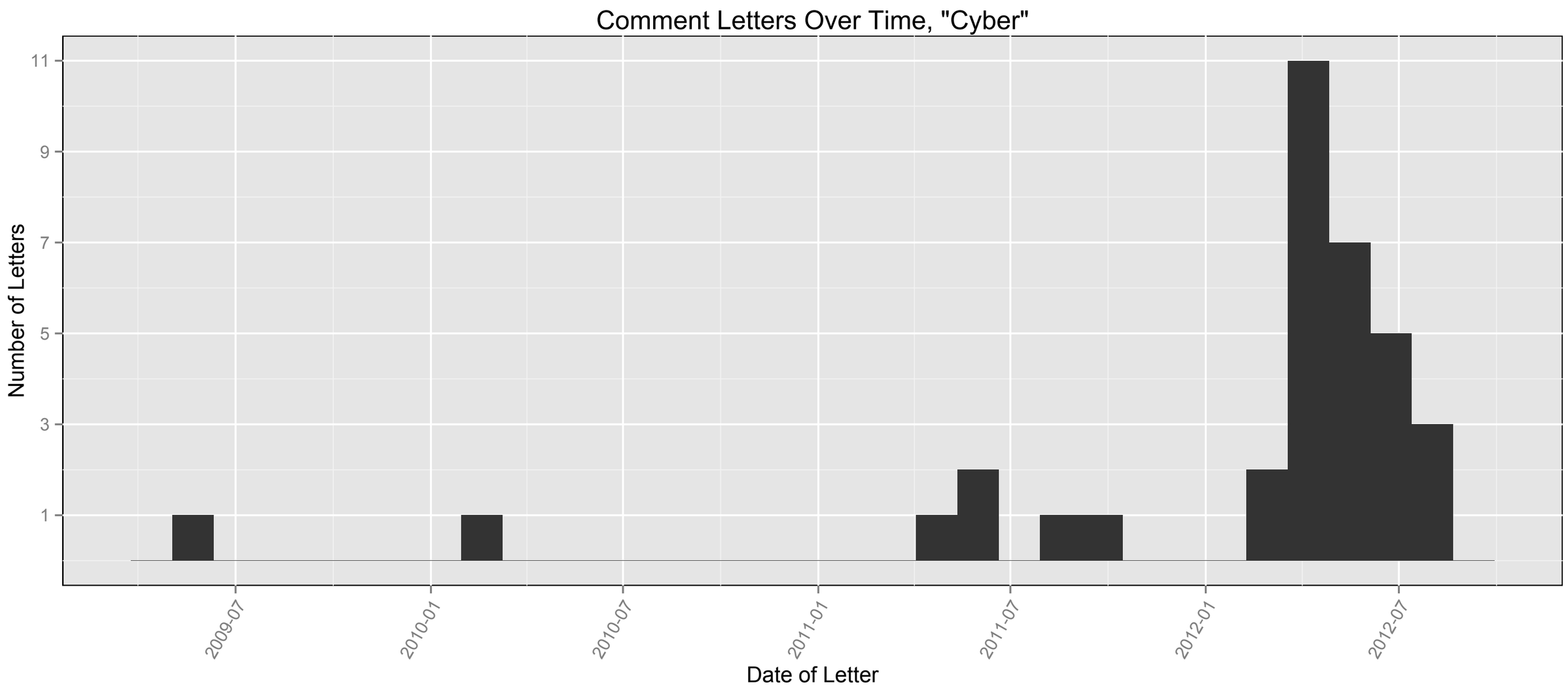
So, how many of these letters are there?



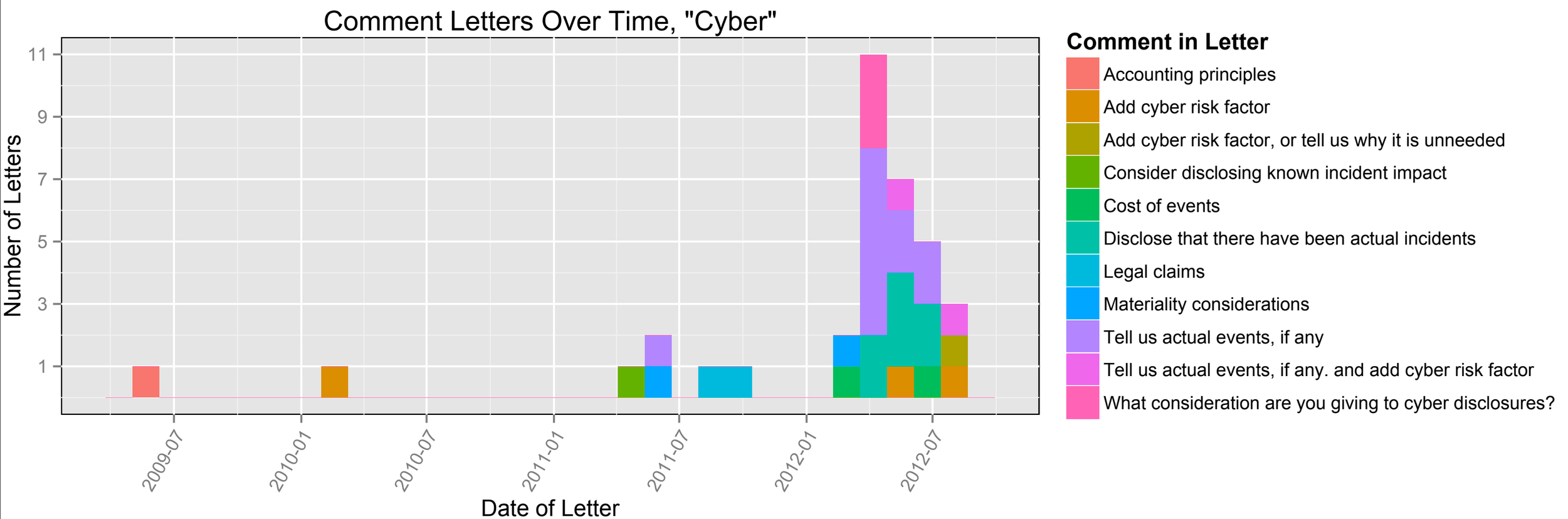
http://searchwww.sec.gov/EDGARFSClient/jsp/EDGAR_MainAccess.jsp

MIRcon 2012

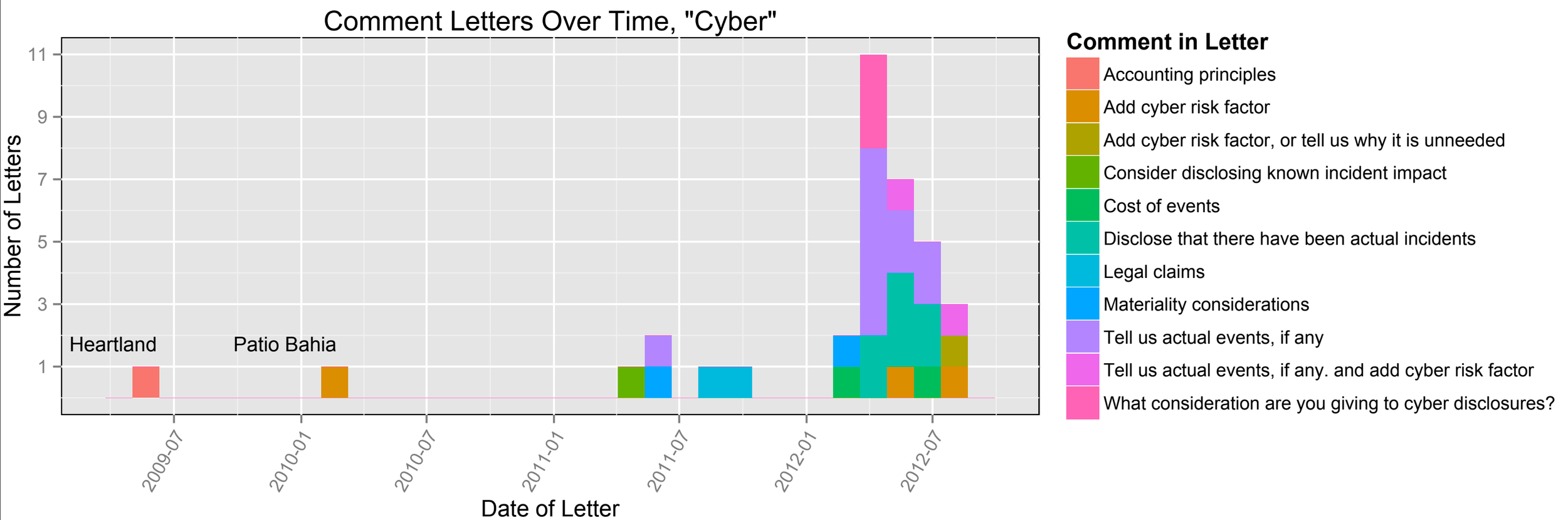
Narrowing to “cyber-” Comment Letters



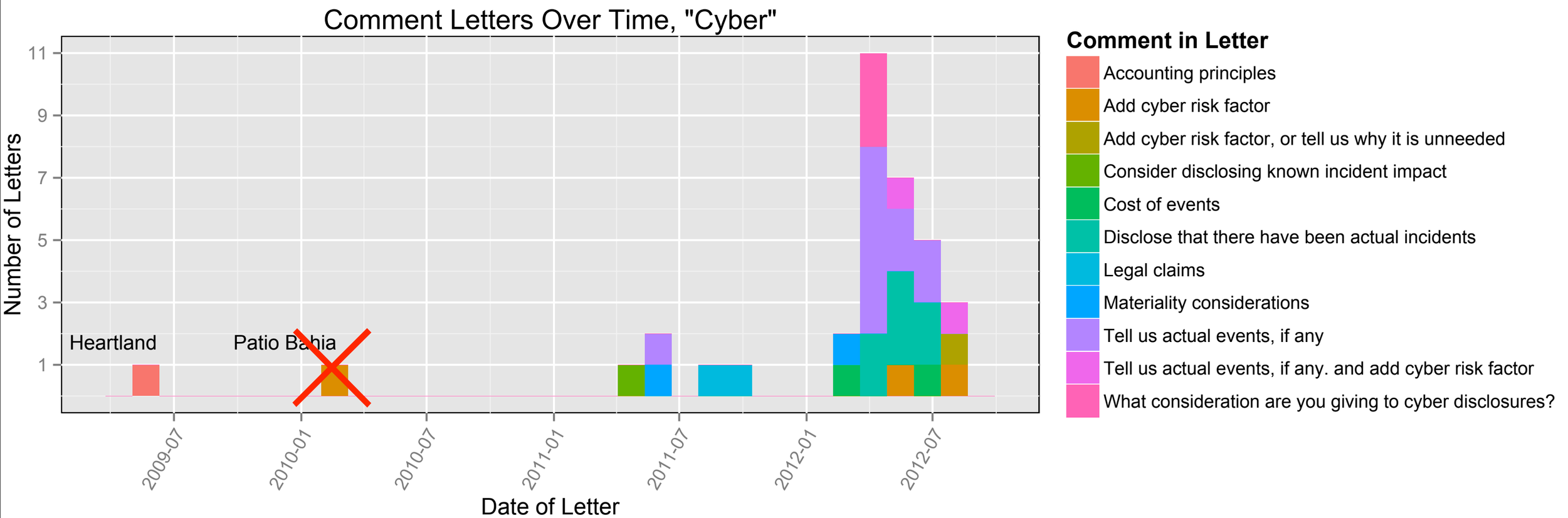
And within them, showing comment type



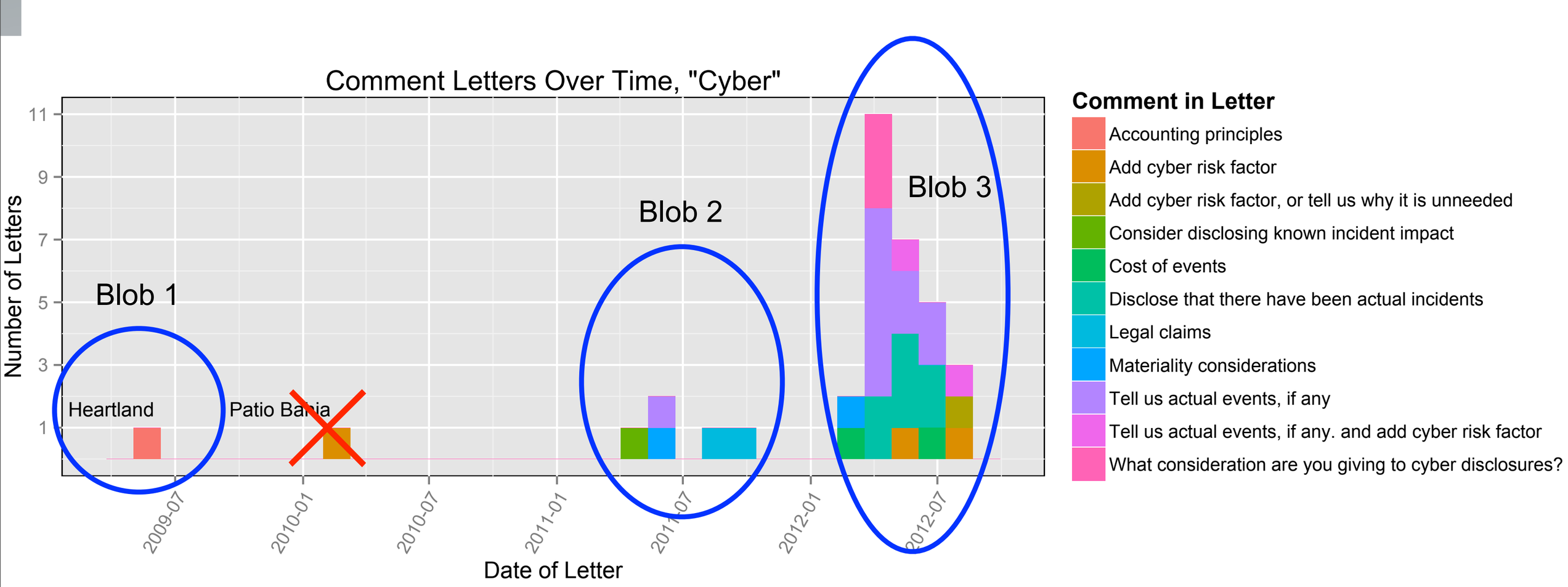
And within them, showing comment type



And within them, showing comment type



And within them, showing comment type



Blob 1: Heartland Payment Systems

Reconciliation of Non-GAAP Financial Measures And Regulation G Disclosure
To supplement its consolidated financial statements presented in accordance with accounting principles generally accepted in the United States ("GAAP"), the Company provides additional measures of it operating results, net income and earnings per share, which exclude certain costs and expenses related to the processing system intrusion. The Company believes that these non-GAAP financial measures are appropriate to enhance understanding of its historical performance as well as prospects for its future performance.

This press release contains non-GAAP financial measures within the meaning of Regulation G promulgated by the Securities and Exchange Commission. Pursuant to Regulation G, a reconciliation of these non-GAAP financial measures with the comparable financial measures calculated in accordance with GAAP for the three months ended March 31, 2009 follows *(In thousands, except per share)*:

Net income (loss) attributable to Heartland	
Non-GAAP – Adjusted net income attributable to Heartland	$ 5,384
Less adjustments:	
Provision for processing system intrusion	12,590
Income tax benefit of provision for processing system intrusion	(4,751)
After-tax provision for processing system intrusion	7,839
GAAP – Net income (loss) attributable to Heartland	$ (2,455)
Diluted earnings (loss) per share	
Non-GAAP – Adjusted net income per diluted share	$ 0.14
Less: provision for processing system intrusion	$ (0.20)
GAAP – Net income (loss) per diluted share	$ (0.06)
Shares used in computing diluted earnings per share	37,842

Form 8-K filed May 7, 2009

8. We note your use of non-GAAP measures in the Form 8-K noted above which excludes certain costs and expenses related to the processing system intrusion. Tell us how you considered Question 8 of Frequently Asked Questions Regarding the Use of Non-GAAP Financial Measures to include the following disclosures:

- the manner in which management uses the non-GAAP measure to conduct or evaluate its business;
- the economic substance behind management's decision to use such a measure;
- the material limitations associated with use of the non-GAAP financial measure as compared to the use of the most directly comparable GAAP financial measure;
- the manner in which management compensates for these limitations when using the non-GAAP financial measure; and
- the substantive reasons why management believes the non-GAAP financial measure provides useful information to investors.

In this regard, we believe you should further enhance your disclosures to comply with Item 10(e)(1)(i)(C) and (D) of Regulation S-K and Question 8 of the related FAQ to demonstrate the usefulness of your non-GAAP financial measures since your current disclosures regarding the reasons for presenting these non-GAAP measures appear overly broad.

Heartland Payment Systems

Reconciliation of Non-GAAP Financial Measures And Regulation G Disclosure

To supplement its consolidated financial statements presented in accordance with accounting principles generally accepted in the United States ("GAAP"), the Company provides additional measures of it operating results, net income and earnings per share, which exclude certain costs and expenses related to the processing system intrusion. The Company believes that these non-GAAP financial measures are appropriate to enhance understanding of its historical performance as well as prospects for its future performance.

Net income (loss) attributable to Heartland	
Non-GAAP – Adjusted net income attributable to Heartland	$ 5,384
Less adjustments:	
Provision for processing system intrusion	12,590
Income tax benefit of provision for processing system intrusion	(4,751)
After-tax provision for processing system intrusion	7,839
GAAP – Net income (loss) attributable to Heartland	$ (2,455)
Diluted earnings (loss) per share	
Non-GAAP – Adjusted net income per diluted share	$ 0.14
Less: provision for processing system intrusion	$ (0.20)
GAAP – Net income (loss) per diluted share	$ (0.06)
Shares used in computing diluted earnings per share	37,842

http://www.sec.gov/Archives/edgar/data/1144354/000119312509102545/dex991.htm

SEC→Heartland Payment Systems

Form 8-K filed May 7, 2009

8. We note your use of non-GAAP measures in the Form 8-K noted above which excludes certain costs and expenses related to the processing system intrusion. Tell us how you considered Question 8 of Frequently Asked Questions Regarding the Use of Non-GAAP Financial Measures to include the following disclosures:

- the manner in which management uses the non-GAAP measure to conduct or evaluate its business;
- the economic substance behind management's decision to use such a measure;
- the material limitations associated with use of the non-GAAP financial measure as compared to the use of the most directly comparable GAAP financial measure;
- the manner in which management compensates for these limitations when using the non-GAAP financial measure; and
- the substantive reasons why management believes the non-GAAP financial measure provides useful information to investors.

In this regard, we believe you should further enhance your disclosures to comply with Item 10(e)(1)(i)(C) and (D) of Regulation S-K and Question 8 of the related FAQ to demonstrate the usefulness of your non-GAAP financial measures since your current disclosures regarding the reasons for presenting these non-GAAP measures appear overly broad.

1 Use

2 Substance

3 Material limitations

4 Compensation for limitations

5 Why useful for investors?

http://www.sec.gov/Archives/edgar/data/1144354/000119312509102545/dex991.htm

1 Use

Management uses these non-GAAP measures to evaluate performance period over period, to analyze the underlying trends in the Company's business, to assess its on-going operating performance relative to its competitors, and to establish operational goals and forecasts. **Costs and expenses related to the Processing System Intrusion are not indicative of the Company's on-going operating performance and are therefore excluded by management in assessing the Company's operating performance, as well as from the measures used for making operating decisions**, although in making operating decisions management is mindful of its need to utilize cash to pay for the costs and expenses relating to the Processing System Intrusion.

http://www.sec.gov/Archives/edgar/data/1144354/000119312509147252/filename1.htm

2 Substance, cont'd

While the Company has determined that the Processing System Intrusion has triggered other loss contingencies, to date **an unfavorable outcome is not believed by it to be probable on those claims that are pending or have been threatened against it**, or that the Company considers to be probable of assertion against it, **and the Company does not have sufficient information to reasonably estimate the loss it would incur in the event of an unfavorable outcome on any such claim**. Therefore, in accordance with SFAS No. 5, "Accounting for Contingencies," no reserve/liability has been recorded as of March 31, 2009 with respect to any such claim, except for fines actually assessed by MasterCard and Visa. As more information becomes available, if the Company should determine that an unfavorable outcome is probable on such a claim and that the amount of such probable loss that it will incur on that claim is reasonably estimable, it will record a reserve for the claim in question. **If and when, the Company records such a reserve, it could be material and could adversely impact its results of operations, financial condition and cash flow.** [Note to Staff: At such time as the Company determines that it has information sufficient to enable it to establish a reserve/liability for such claim this disclosure will be revised in the Company's future filings with the SEC to describe such reserve/liability and the amount thereof.]

Additional costs the Company expects to incur for investigations, remedial actions, legal fees, and crisis management services related to the Processing System Intrusion will be recognized as incurred. Such costs are expected to be material and could adversely impact the Company's results of operations, financial condition and cash flow.

http://www.sec.gov/Archives/edgar/data/1144354/000119312509147252/filename1.htm

5 Why useful for investors?

The Company believes that presenting non-GAAP net income and non-GAAP earnings per share that exclude the impact of the Provision for Processing System Intrusion in addition to the related GAAP measures provides investors greater transparency to the information used by the Company's management for its financial and operational decision-making and allows investors to see the Company's results through the eyes of management. Additionally, the Company believes that the inclusion of these non-GAAP financial measures provides enhanced comparability in its financial reporting. The Company further believes that providing this information better enables its investors to understand the Company's operating performance and underlying business fundamentals, and to evaluate the methodology used by management to evaluate and measure such performance.

http://www.sec.gov/Archives/edgar/data/1144354/000119312509147252/filename1.htm

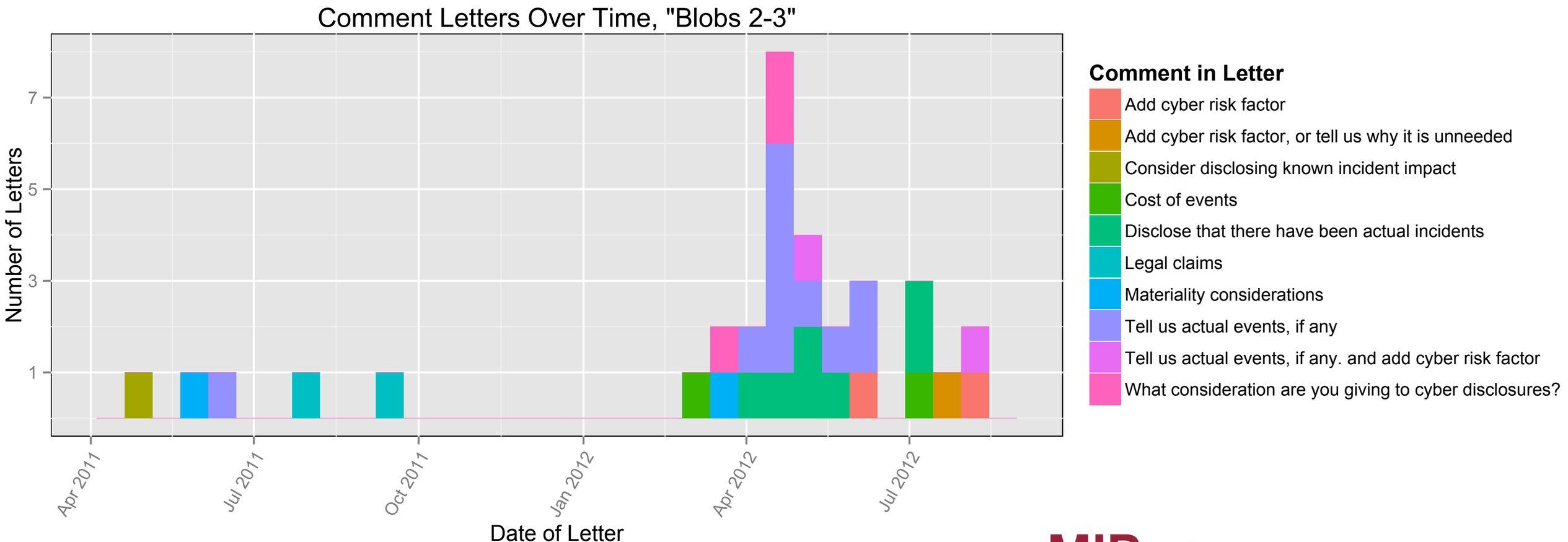
Blob 1: Summary

This comment letter focuses exclusively on the accounting treatment given to costs and expenses which happen to derive from an intrusion.

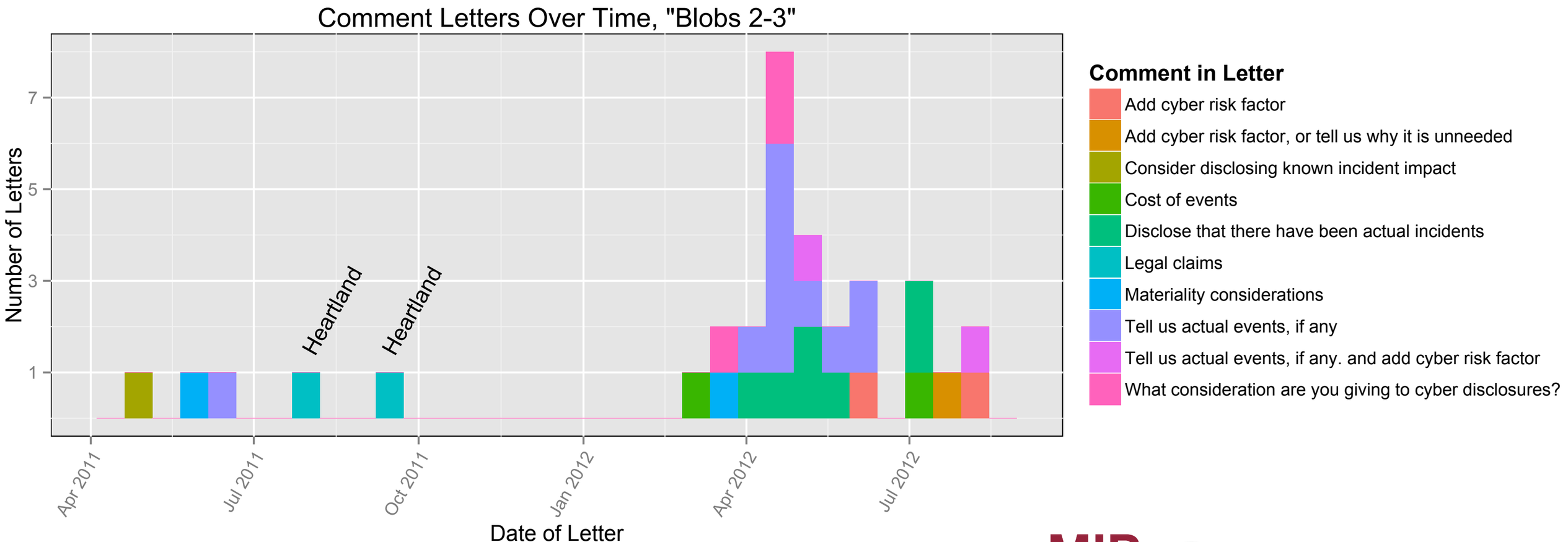
The manner in which the firm estimates (or cannot estimate) legal costs is illuminating, and provides an intriguing glimpse into the world of likelihood determination under uncertainty as it is practiced by CPAs and lawyers.

If “cyber risk” and “cyber incidents” are perceived as increasingly important, this is a world in which today’s information security management must be able to operate.

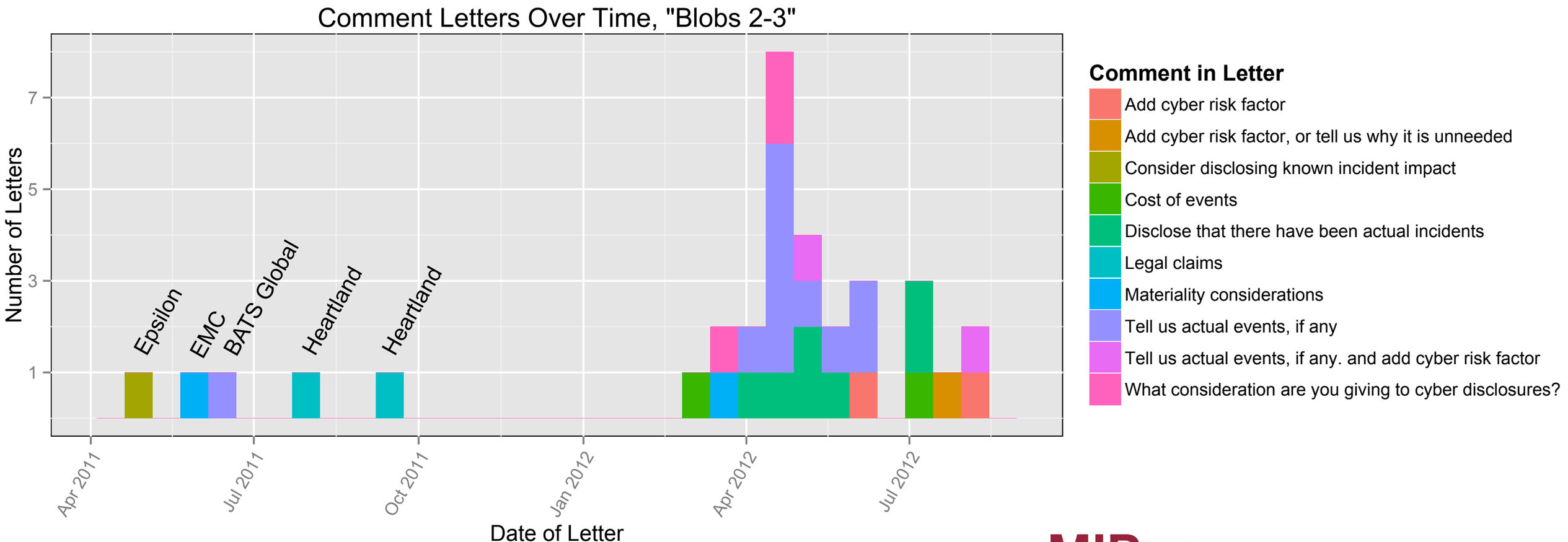
Blob 2: Transitional Period?



Blob 2: Transitional Period?



Blob 2: Transitional Period?



Alliance Data (Epsilon)

Alliance Data Systems, is the parent company of Epsilon, which suffered a large data breach*:

"We note that your Epsilon business was recently attacked by cyber-thieves. In your next quarterly report on Form 10-Q, ensure that you consider disclosing and quantifying any reasonably expected material impact on your liquidity, capital resources and/or results of operations from any currently known trends, events and uncertainties related to this incident"**

Here, the SEC asks for the firm *consider* adding language to its next quarterly report, in the MD&A section. As with Heartland, this is a focus on the pure accounting aspect of the incident: "How might it affect the numbers", in other words, as opposed to whether it provides additional information about the riskiness or degree of speculativeness of an investment.

* http://datalossdb.org/incidents/3540-names-and-email-addresses-exposed-in-third-party-email-service-provider-breach
**http://www.sec.gov/Archives/edgar/data/1101215/000000000011027848/filename1.pdf

EMC

Please update us as to the status of the cyber attack mounted against RSA. In this regard, **you indicated in the March 17, 2011 Form 8-K that based on what you knew at such time, the company did not believe such matter will have a material impact on your financial results. Please tell us if you still believe that to be true.** In addition, you indicated that the company took a variety of "aggressive measures" against the threat to protect your business, including further hardening your IT infrastructure. **Tell us what other measures, if any, you have taken and tell us how the costs incurred to implement such measures impacted your first quarter results of operations. In addition, tell us how you considered including a discussion of this attack in your March 31, 2011 Form 10-Q.**

This is partially along "pure accounting" lines, *but with the SEC asking for insight into the company's thinking* about what (if anything) to disclose in their 10-Q.

BATS Global Markets

And finally, a Comment Letter to BATS Global Markets (in the “Security & Commodity Brokers, Dealers, Exchanges & Services” industrial classification):

“We note the risks regarding your vulnerability to unauthorized access, computer viruses, and inadvertent disclosure of confidential information. **Please disclose any significant instances of such events.**”

Very interesting that this request for specific disclosure or actual incidents came in June, 2011 BEFORE the revised guidance was issued.

I would argue that this comment letter is the Patient Zero of what I’ve called the Emerging New Normal disclosure regime.

Blob 2: Summary

- Still an interest, of course, in “pure accounting”
- Starting to become curious about registrant reasoning about materiality
- Leading edge of specific incident disclosure requirement begins to emerge

Blob 3: Some simple statistics

Summary of SEC Comment	Number of Letters	
	Initial	Followup
Tell us actual events, if any	8	2
Disclose that there have been actual incidents	3	3
What consideration are you giving to cyber disclosures?	3	0
Add cyber risk factor	2	0
Cost of events	1	1
Tell us actual events, if any. and add cyber risk factor	2	0
Materiality considerations	1	0
Add cyber risk factor, or tell us why it is unneeded	1	0

Firms asked to divulge incidents, if any

Firm	Industry
Hartford Financial Services Group	Insurance
Aon Corp	Insurance
City National Corporation	Commercial Banking
Ameriprise Financial	Investment Advice
CIT Group	Finance Lessors
Eli Lilly	Pharmaceutical Preparations
Quest Diagnostics	Medical Laboratories
Walmart	Retail

Looks from this that they're Insurance and Financial Services, Pharmaceutical and Medical, and the biggest private employer in the country.

MIRCon 2012

Nucor

April 23, 2012: SEC writes...

We note that you state that the steelmaking business is subject to numerous inherent risks, particularly unplanned events such as explosions, fires, other accidents, natural or man-made disasters, acts of terrorism, inclement weather and transportation interruptions. **Please advise us whether your business is also subject to risks associated with cyber attacks or information technology system failures. If so, please tell us what consideration you are giving to including these unplanned events in this risk factor disclosure.**

Firm responds, and on June 6, SEC writes:

In response to comment one of our letter dated April 23, 2012, you state that ...you do not believe that the risk to an investment in Nucor relating to your information technology systems, including potential cyber attacks or failures, is significantly different from the same risks faced by an investor in most manufacturing and other comparable businesses operating in the United States today. **Please advise us of your experience with any cyber incidents in the past and any consequences that you have suffered.**

Hartford

April 5, 2011: SEC writes...

You disclose that your business is highly dependent on your ability, and the ability of certain third parties, to access certain systems to perform necessary business functions. We note that you also disclose that your systems and the systems of third parties may be subject to a computer virus or other malicious code, unauthorized access, a cyber attack or other computer related violation. **Please tell us whether you have experienced a virus or other malicious code, unauthorized access, a cyber attack or other computer related violation in the past** and, if so, whether disclosure of that fact would provide the proper context for your risk factor disclosures.

Firm responds, and on May 7, SEC writes:

You state that **you have not experienced a material breach of cybersecurity. Your response does not appear to address whether you are experiencing any potential current business risks concerning cybersecurity. For example, despite the fact you believe you have not experienced a material breach of your cybersecurity, are you currently experiencing attacks or threats to your systems? If you have experienced attacks in the past, please expand your risk factor in the future to state that.**

Aon

April 12, 2012: SEC writes...

You disclose that you rely on the efficient and uninterrupted operation of complex information technology systems and networks. You also disclose that all information technology systems are potentially vulnerable to damage or interruption from a variety of sources, including computer viruses and security breaches, among others. **Please tell us whether you have experienced a computer virus, security breach, cyber attack or other computer related violation in the past.** If you have experienced these types of events, **tell us what consideration you gave to tailoring your risk factor disclosure to more clearly state that you have been subject to attacks in the past and to highlight the potential consequences of the types of attacks that are most concerning to you.**

City National

April 23, 2012: SEC writes...

Furthermore, we note reports that the prevalence of cyber attacks, including attacks that have resulted in the loss of customer data, have increased. For instance, in the past two years, a number of financial institutions, or service providers to financial institutions, have been the victim of hacking incidents which have compromised the information of a large number of customers. **Please tell us whether you have experienced any attacks, viruses, intrusions or similar problems in the past and management's view of the impact of any such attacks on your operations, expenses and risks.**

Quest Diagnostics

SEC makes familiar “We note.....please tell us....”.

We note that you state that your IT systems may be subject to physical or electronic intrusions, computer viruses, unauthorized tampering and similar disruptive problems. Given your extensive use of information technology systems, please tell us whether you have experienced any attacks, viruses, intrusions or similar problems in the past and, if so, whether disclosure of that fact would provide the proper context for your risk factor disclosures

Firm responds April 30, 2011:

The Company respectfully advises the Staff that the Company’s information technology systems have not sustained any attacks, viruses, intrusions or similar problems that have materially disrupted, interrupted, damaged or shutdown the Company’s information.

SEC replies on May 15, 2011:

...please tell us whether you have experienced <u>any</u> attacks, viruses, intrusions or similar problems in the past. If so, your disclosure in future filings should not be limited to stating that you “may” experience such attacks, viruses, intrusions or similar problems. In order to provide the proper context, **you should clearly state that you have experienced attacks** and you may include language that indicates that the attacks were mitigated.

Request to disclose known incidents

- Western Union
  - In your response to comment one in our letter dated March 21, 2012, **you state that you have been the subject of cyber attacks.** You also clarify that the attacks are primarily aimed at interrupting your business or exploiting information security vulnerabilities. In order to place the risks described in this risk factor in an appropriate context, **please expand your risk factor to disclose this information.**
- Google
  - **We also note your Current Report on Form 8-K filed January 13, 2010 disclosing that you were the subject of a cyber attack. In order to provide the proper context for your risk factor disclosures, please revise your disclosure in your next quarterly report on Form 10-Q to state that in the past you have experienced attacks.**
- Eastman Chemical
  - we note that **your response suggests that you have in fact experienced third-party breaches of your computer systems. In order to place the risks described in your current risk factor in appropriate context, in future filings please expand your disclosure to state that you have experienced cyber attacks and breaches**

Tell us actual events, if any. Add risk factor.

- Hancock Holding Company
  - **We note that none of your risk factors provides a separate discussion of the risks posed to your operations from your dependence upon technology or to your business**, operations or reputation from the loss or compromise of customer information. We also note that the incidences of cyber attacks, including upon financial institution or their service providers, have increased over the past year. In future filings, beginning with your next Form 10-Q, **please provide risk factor disclosure describing the cybersecurity risks that you face.** In addition, **please tell us whether you have experienced cyber attacks in the past.** If so, please also disclose that you have experienced such cyber attacks in order to provide the proper context for your risk factor disclosure.

- Wynn Las Vegas
  - **We note that none of your risk factors, or other sections of your Form 10-K, specifically address any risks you may face from cyber attacks....**We note press reports that hotels and resorts are increasingly becoming a target of cyber attacks. Beginning with your next Form 10-Q, please provide risk factor disclosure describing the cybersecurity risks that you face. If you have experienced any cyber attacks in the past, please state that fact in the new risk factor in order to provide the proper context.

Blob 3: Summary

- Requests for incident history now common
- Absence of “cyber-” risk factor raises eyebrows, especially in some industries
- Immateriality does not preclude disclosure

Related Work

Joseph Menn, “Exclusive: Hacked companies still not telling investors”, Reuters, Feb 2, 2012
http://www.reuters.com/article/2012/02/02/us-hacking-disclosures-idUSTRE8110YW20120202

Linda Sandler, “SEC Guidance on Cyber-Disclosure Becomes Rule for Google“, Bloomberg News, Aug 29, 2012
http://www.businessweek.com/news/2012-08-29/sec-guidance-on-cyber-disclosure-becomes-rule-for-google

Linda Sandler, “The SEC Says Speak Up About Hack Attacks“, Bloomberg News, Sept 6 2012,
http://www.businessweek.com/articles/2012-09-06/the-sec-says-speak-up-about-hack-attacks

Questions

?