The SEC Guidance on Cybersecurity and Incident Disclosure: What You Need to Know

Thursday, August 9, 2012
11 – 12:30 p.m. EDT
Welcome & Introductions

Moderator:
Melissa J. Krasnow, CIPP/US, Partner, Dorsey & Whitney LLP
Welcome & Introductions

Panelists:

Lisa Beth Lentini, Senior Director, Global Compliance, Carlson Wagonlit Travel

Liza Mark, Partner, Dorsey & Whitney LLP

Wayne Matus, Partner, Pillsbury Winthrop Shaw Pittman LLP

www.privacyassociation.org
Program Outline

I. Big picture considerations
II. U.S. federal securities laws
III. Background about the SEC guidance
IV. SEC guidance
V. Examples of actual SEC filing disclosures
VI. SEC comments about SEC filing disclosures – Amazon.com example
VII. Convergence with incident/breach notification & security procedures
VIII. Implications
IX. Steps public companies can take
X. Resources
XI. Questions & Answers
Big picture considerations
Big picture considerations

- State breach notification laws
- HIPAA / HITECH Act
- Foreign breach notification laws
- State, federal and foreign security procedures laws
- FTC guidance
- SEC disclosure guidance
- State enforcement
- Federal enforcement
- Foreign enforcement
- Litigation
- Cybersecurity legislation
- Cyber liability insurance
- Company policies and procedures
U.S. federal securities laws
U.S. federal securities laws

• U.S. Securities and Exchange Commission’s (SEC’s) mission is to:
  - protect investors,
  - maintain fair, orderly and efficient markets and
  - facilitate capital formation
U.S. federal securities laws

• In furtherance of its mission, one of the major functions of the SEC is to:
  – ensure that there is sufficient and accurate public disclosure about the current status of the public companies and
  – ensure that the disclosures are widely disseminated (i.e., disclosure is not selective only to a favored few)
U.S. federal securities laws

• U.S. public companies have periodic filing obligations where they are required to address the market

• When they do address the market, they need to be both accurate in what they tell the market and not omit any information that would make the picture presented to the market materially misleading
U.S. federal securities laws

• The periodic filing obligations are:
  – 10-K annual report – required every year
  – 10-Q quarterly reports – required every quarter
  – 8-K current report – required for certain specified events that materially affect the company
  – proxy statement – required generally every year to provide information for the general shareholders’ meeting
U.S. federal securities laws

• Other situations where the public company needs to address the market – when they sell securities into the market:
  – S-1 registration statement
  – S-3 registration statement
U.S. federal securities laws

- Disclosure of timely, comprehensive and accurate information about risks and events that a reasonable investor would consider important to an investment decision

- Public access to these SEC filings at the SEC website at [www.sec.gov](http://www.sec.gov)
Background about the SEC guidance
Background about the SEC guidance

• Within the last 2 years, cybersecurity has become a major concern, both on the national security front and on a commercial front:
  – increased levels of cybersecurity attacks
  – proposed legislation on cybersecurity and
  – increased media coverage about cybersecurity as a threat
Background about the SEC guidance

• 5 senators sent a letter to SEC Chairman Mary Schapiro on May 11, 2011, discussing the cybersecurity threat and urging the SEC to provide interpretive guidance to clarify existing disclosure requirements pertaining to information security risk, including material information security breaches involving intellectual property or trade secrets. Some have pointed to this letter as the genesis of the SEC guidance.
Background about the SEC guidance

- The SEC regularly reviews and comments on the public disclosure of public companies

- The SEC tries to review every public company’s SEC filings at least once every 3 years
Background about the SEC guidance

• In the course of these reviews, the SEC comments on this disclosure and often uses the comment process as a means of having the public company change their disclosure.

• The SEC is stepping up its efforts to comment on cybersecurity related disclosure, which implies that they are focused on the disclosure in this area.
SEC guidance
SEC guidance

• The SEC is a somewhat unique organization in that there are often times Staff Legal Bulletins to clarify Corporation Finance positions on issues

• Corporation Finance Staff at the SEC issued the Division of Corporation Finance’s Disclosure Guidance Topic No. 2 – guidance about disclosure of cybersecurity risks and cyber incidents in October 2011 for public companies

• How it works:
  – lays out how the SEC applies the current rules to the issue of cybersecurity
  – no changes to existing SEC rules and regulations
SEC guidance

1. risk factors
   - evaluate cybersecurity risks and consider previous cyber incidents (including severity and frequency), the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks (including the potential costs and other consequences)
   - consider the adequacy of preventative actions taken to reduce cybersecurity risks relative to the industry of the public company and risks to that security, including threatened attacks of which the public company is not aware
SEC guidance

1. risk factors
   - disclose if among the most significant factors that make an investment in the company speculative or risky
   - adequately describe the nature of the material risks and specify how each risk affects the particular public company
   - avoid generic risk factor disclosure
   - however, disclosure is not required where it would compromise public company’s cybersecurity
SEC guidance

2. management’s discussion and analysis (MD&A) of financial condition and results of operations
   - if costs or other consequences associated represent a material event, trend or uncertainty that is reasonably likely to have a material effect on public company’s results of operations, liquidity or financial condition or that would cause reported financial information not to be necessarily indicative of future operating results or financial condition

3. description of business if materially affects its products, services, relationships with customers or suppliers or competitive conditions
SEC guidance

4. legal proceedings where a party to a material pending legal proceeding that involves a cyber incident / breach (e.g., material litigation)

5. disclosure controls and procedures where pose a risk to the public company’s ability to record, process, summarize and report information required to be disclosed in SEC filings

   – consider whether there are any deficiencies in disclosure controls and procedures that would render them ineffective
SEC guidance

6. financial statement disclosure

– must provide certain disclosures of losses that are at least reasonably possible
– where cyber incident is discovered after the balance sheet date but before the issuance of financial statements, consider disclosure of a recognized or nonrecognized subsequent event
Examples of actual SEC filing disclosures
Examples of actual SEC filing disclosures

Excerpt from VeriSign risk factor disclosure in Form 10-Q filed 10/28/11 about 2010 security breaches that previously had not been disclosed in SEC filings:

*We experienced security breaches in the corporate network in 2010 which were not sufficiently reported to Management.*

....The occurrences of the attacks were not sufficiently reported to the Company’s management at the time they occurred for the purpose of assessing any disclosure requirements. Management was informed of the incident in September 2011 and, following the review, the Company’s management concluded that our disclosure controls and procedures are effective. However, the Company has implemented reporting line and escalation organization changes, procedures and processes to strengthen the Company’s disclosure controls and procedures in this area....
Examples of actual SEC filing disclosures

• The SEC guidance applies uniformly to both U.S. and non-U.S. public companies

• However, non-U.S. public companies may be subject to local privacy and other disclosures
Examples of actual SEC filing disclosures

Excerpt from Sony financial information disclosure in Form 20-F (Amendment No. 1) filed 7/20/12 regarding PlayStation cyber attack:

Legal Proceedings

….Beginning in early 2011, the network services of PlayStation®Network, Qriocity™, Sony Online Entertainment LLC and websites of other subsidiaries came under cyber-attack. As of June 27, 2012, Sony has not received any confirmed reports of customer identity theft issues or misuse of credit cards from such cyber-attacks. However, in connection with certain of these matters, Sony has received inquiries from authorities in a number of jurisdictions, including orders for reports issued by the Ministry of Economy, Trade and Industry of Japan as well as the Financial Services Agency of Japan, formal and/or informal requests for information from Attorneys General from a number of states in the United States and the U.S. Federal Trade Commission, various U.S. congressional inquiries and others. Additionally, Sony Corporation and/or certain of its subsidiaries have been named in a number of purported class actions in certain jurisdictions, including the United States. Based on the stage of these inquiries and proceedings, it is not possible to estimate the amount of loss or range of possible loss, if any, that might result from adverse judgments, settlements or other resolution of all of these matters.
SEC comments about SEC filing disclosures – Amazon.com example
SEC comments about SEC filing disclosures – Amazon.com example

Excerpt from Amazon.com response to SEC comment letter filed 4/9/12 regarding Form 10-K filed 2/1/12

Item 1A. Risk Factors, page 5

We Could Be Harmed by Data Loss or Other Security Breaches, page 10

1. We note that Zappos.com announced on its website that a cyber attack occurred during which millions of user accounts were compromised.
Please tell us what consideration you gave to including expanded disclosure consistent with the guidance provided by the Division of Corporation Finance’s Disclosure Guidance Topic No. 2. In particular, in light of the fact that your subsidiary has actually experienced this cyber attack (as opposed to warnings that you may experience such an attack), please address whether disclosure of the breaches would provide the proper context for this risk factor disclosure and whether the potential harm to your business resulting from these and similar breaches should be expanded to address reputational damage affecting customer or investor confidence.
In January 2012, Zappos.com experienced a cyber attack, which resulted in illegal access to data about Zappos’ approximately 24 million Zappos customer accounts. Full credit card numbers were not accessed. The data accessed included customer names, e-mail addresses, billing and shipping addresses, phone numbers, credit card type, the last few digits of credit card numbers and expiration dates (i.e., the standard information found on receipts), and/or cryptographically scrambled passwords (but not actual passwords).
We evaluated this matter prior to filing the 2011 10-K, including the nature of the breach, and determined that, in light of our disclosures in the risk factor “We Could Be Harmed by Data Loss or Other Security Breaches,” information on the specific incident would not provide investors with additional material information relating to the cyber attack risks facing our business. We supplementally advise the Staff that this incident did not have a material impact on Amazon’s business, as Zappos is not material to our consolidated revenues. In addition, we believed that, due to the nature of the cyber attack, any impact on Zappos’ business would be transitory, and in fact, within approximately one month after the cyber attack, revenue growth at Zappos had returned to the growth levels experienced immediately prior to the cyber attack.
SEC comments about SEC filing disclosures – Amazon.com example

2. We note that you rely on third party technology and systems in certain aspects of your business, including for encryption and authentication technology to securely transmit confidential information. Please explain to us how these technologies and systems fit into your business operations and describe the associated risks.
Response

We use third party encryption and authentication technology, including hardware and software solutions, to control access to and protect data within the Company. We also use third party encryption software and hardware to provide secure remote access to our internal corporate networks for our employees (as part of our Virtual Private Network (VPN)) and to allow secure access by our customers to some of our services, customer data, and limited customer account information. Encryption is used to secure sensitive information when it is in transit or being stored. We have implemented policies and internal controls to protect sensitive information, applying more stringent security measures as the sensitivity of the information increases. We have also implemented compensating controls to minimize the risk of loss or misuse of confidential information in the event of a security breach at a third party vendor. In future filings, we will revise our disclosure in the risk factor captioned “We Could Be Harmed by Data Loss or Other Security Breaches” to read as follows:
“As a result of our services being web-based and the fact that we process, store and transmit large amounts of data, including personal information, for our customers, failure to prevent or mitigate data loss or other security breaches could expose us or our customers to a risk of loss or misuse of such information, adversely affect our operating results, result in litigation or potential liability for us and otherwise harm our business. In addition, we rely on third party technology and systems in certain aspects of our businesses, including for encryption and authentication technology to securely transmit confidential information. Although we have developed systems and processes that are designed to protect customer information and prevent data loss and other security breaches, including systems and processes designed to minimize the impact of a security breach at a third party vendor, such measures cannot provide absolute security.”
SEC comments about SEC filing disclosures – Amazon.com example

Amazon.com risk factor disclosure in Form 10-Q filed 7/27/12, showing changes from Form 10-K filed 2/1/12 and Form 10-Q filed 4/27/12

*We Could Be Harmed by Data Loss or Other Security Breaches*
As a result of our services being web-based and the fact that we process, store and transmit large amounts of data, including personal information, for our customers, failure to prevent or mitigate data loss or other security breaches, including breaches of our vendors’ technology and systems, could expose us or our customers to a risk of loss or misuse of such information, adversely affect our operating results, result in litigation or potential liability for us and otherwise harm our business. We use third party technology and systems for a variety of reasons, including, without limitation, encryption and authentication technology, employee email, content delivery to customers, back-office support and other functions. Some subsidiaries had past security breaches, and, although they did not have a material adverse effect on our operating results, there can be no assurance of a similar result in the future. Although we have developed systems and processes that are designed to protect customer information and prevent data loss and other security breaches, including systems and processes designed to reduce the impact of a security breach at a third party vendor, such measures cannot provide absolute security.
Convergence with incident/breach notification and security procedures

- Amazon.com / Zappos.com
- Incident/breach notification required by law or otherwise made (e.g., business reasons, public relations, etc.)
- Security procedures
- Risk assessment
- Enforcement
Implications

• Public companies are walking a fine balancing act
• SEC guidance may require disclosure of any cybersecurity incidents / breaches if the effect of such breach is material to the public company
• Failure to disclose in the SEC filings could result in:
  – plaintiff’s class action lawsuit for inaccurate or misleading disclosure or
  – SEC enforcement proceedings
• On the other hand, extensive disclosure may encourage lawsuits for the incident/breach itself
• Public relations/media
Steps public companies can take
Steps public companies can take:

- consider cybersecurity and cyber incidents as part of overall risk framework
- communicate and collaborate with the people responsible for disclosure
- conduct a risk assessment
- review applicable company policies and agreements, procedures and practices
- review insurance coverage relating to cybersecurity and cyber incidents, if any; other mechanisms
- assess whether SEC filing disclosure about cybersecurity risks and cyber incidents is adequate now and on an ongoing basis (e.g., actual or possible incident / breach)
- coordinate different areas that are involved, including legal, accounting, privacy, information technology, risk management/insurance and corporate communications
Steps public companies can take:

- Informing the board of directors and management
- Functions of board of directors and management
- Coordination of internal functions:
  - person in charge of handling an incident/breach needs to be connected to the person drafting the risk factor – the SEC is no longer satisfied with boilerplate language about potential incident/breach
  - person in charge of handling an incident/breach needs to coordinate with person who manages the public company’s disclosure to make sure that the incident/breach notifications conform, both in timing and content, with the disclosure obligations under the U.S. federal securities laws
  - person in charge of internal controls and procedures needs to coordinate with IT to make sure that those two functions work together
  - person in charge of risk management needs to be coordinated with the IT function
Resources:

Questions & Answers

Contact:

Melissa Krasnow  
krasnow.melissa@dorsey.com

Lisa Beth Lentini  
LLentini@Carlsonwagonlit.com

Liza Mark  
mark.liza@dorsey.com

Wayne Matus  
wayne.matus@pillsburylaw.com
Web Conference Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here:

IAPP Web Conference Participant Feedback Survey

Thank you in advance!

For more information: www.privacyassociation.org
Thank you to our Speakers and Participants
Upcoming IAPP Events:

Live Events:

• **IAPP Privacy Academy 2012**
  San Jose, CA October 10 – 12

• **IAPP Practical Privacy Series 2012**
  New York, NY October 29 – 30
  Washington, DC December 3 - 4

Web Events:

• **Are You a Business Associate?**
  Broadcast Date: Thursday, August 16th
  11:00 am – 12:30 p.m. EDT

For more information:
www.privacyassociation.org
• **Attention IAPP Certified Professionals:**
  This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your CIPP/US, CIPP/G, CIPP/C, CIPP/E or CIPP/IT credential worth 1.5 credit hours. IAPP-certified professionals who are the named participant of the registration will automatically receive credit. If another certified professional has participated in the program but is not the named participant then the individual may submit for credit by submitting the continuing education application form at [www.privacyassociation.org](http://www.privacyassociation.org).

• **Continuing Legal Education Credits:**
The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body’s rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers 60 or 90 minutes of programming.
For questions on this or other IAPP Web Conferences please contact:

Dave Cohen, CIPP/US
Knowledge Manager
International Association of Privacy Professionals (IAPP)
Dave@privacyassociation.org
603.427.9200 x 221