Association of Corporate Counsel

This Webcast Will Begin Shortly

If you have any technical problems with the Webcast or the streaming audio, please contact us via email at:

webcast@acc.com

Thank You!

Planning and Response: Surviving a Data Breach

July 22, 2010

Presented By:

Demetrios Eleftheriou
Senior Counsel – Privacy, EMC Corporation

Jennifer Kashatus, Attorney, Womble Carlyle Sandridge & Rice PLLC

Jill Girardeau, Attorney, Womble Carlyle Sandridge & Rice PLLC

www.acc.com

Definition of a Data Breach

- Unintentional release of confidential, protected, or sensitive data, including:
  - Personally identifiable information (PII) – definition varies by state, but generally includes SSN standing alone and name plus one identifier, such as account information;
  - Personal Health Information (PHI); and
  - Trade Secrets or intellectual property

How a Data Breach Occurs

- Lost device (*e.g.*, laptop, PDA) with unencrypted information – currently represents approximately 36% of data loss incidents
- Third-party errors
- Internal company errors/human error (*e.g.*, inappropriate security of information, process problems – throwing out data in a dumpster, software malfunctions)
- Malicious attacks (hackers) – incidents of malicious attacks are on the rise
- *Data breaches are not limited to large companies*

Monetary Costs of a Data Breach

- Data breaches are expensive
  - 2009: Average cost of data breach increased from $6.65 million to $6.75 million per company
  - To date, most expensive breach event cost a company more than $30 million
- Costs include, but are not limited to, investigating the data breach, notifying consumers and state regulators about the breach, attorney fees and increased staff costs, and fines

Ramifications of Data Breach

- Costs (as stated above)
- Regulatory scrutiny: law enforcement, state attorneys general, Federal Trade Commission
- Potential for fines – not limited to large companies or extensive record loss
  - State AGs have imposed fines due to delayed notification (*see, e.g.,* CS Stars, LLC (NY AG) – stolen laptop; company delayed seven weeks in notifying business owner about the breach; settlement included $60,000 payment)
- Loss of customers

Preparation is Critical to Surviving a Data Breach – Create a Plan

- Know the law in your jurisdiction and where you have customers
- Implement a data breach incident response plan
  - Critical that your company can respond promptly in the event of a data breach
  - Some states have fined companies for failing to notify data subjects in a timely manner
- Ensure that the plan will work for your particular company; no one-size-fits-all approach
  - Point of contact
  - Means of reporting breaches/suspected breaches (consider portal for reporting breaches)
- Obtain sign-off of the data breach plan from management before a data breach occurs

Preparation – Communication/Training

- Communicate existence of the plan and contact information to *all* employees
- Train employees/independent contractors
- Repeat training
- Monitor plan; fix what isn't working

Preparation – Third Party Vendors

- Think before your company sends data to a third party – can the third party perform the contracted services without PII
- Contractually protect company – assume the worst and address data breach obligations in contract
  - Control data sent to third party
  - Contractually limit the third party's use, access, and sharing of data
  - Require third party to notify company in the event of a breach/suspected breach, even if the company still is gathering information

Data Security Breach: Overview of an In-House Plan

1. Data Security Breach Decision Tree
   - Legal requirements
   - Contractual requirements
   - Policy considerations
   - Gathering the facts
2. Data Security Breach Notification Plan
   - Key players
3. Final Thoughts

1. Decision Tree: Legal

- Legal requirements
  - 40+ states (no comprehensive US federal law)
  - FFIEC Guidance (GLBA)
    - Financial info
  - HIPAA/HITECH
    - Health info
  - Foreign
  - Different requirements
    - Harm threshold, PII definition, timing of notice, etc.

1. Decision Tree: Contract

- Contractual requirements
  - Obligation on you or third party?
  - How is PII defined?
  - Timing of notice
    - Immediately, promptly or within "X" number of days
  - Content of notice
  - Who will notify?
    - Individuals, regulators, CRAs, or law enforcement
  - Remediation steps

1. Decision Tree: Policy

- Policy considerations
  - Notification is not legally required in any jurisdictions
    - Acquisition and compromise but fraud or misuse is unlikely
      - Notify?
  - Notification is legally required in some jurisdictions
    - State by state or country by country
      - Notify all individuals?
        - » Domestically? Globally?

1. Decision Tree: Gather the Facts

First Step – Is notification to the individual necessary?

Some questions to ask:

- Where did the breach happen?
  - Internal
  - Service provider
  - Third party
- When did the breach happen?
- Who owns the data involved in the breach?

1. Decision Tree: Gather the Facts

- Data elements involved in the breach?
  - Name + credit card or SSN, etc.
- Was the data encrypted?
  - Encryption key accessed?
- Was the data acquired or is there a reasonable belief that the data was acquired?
  - Compare to mere “access” to the data.
  - Has “misuse” occurred or is it “reasonably likely” that the misuse will occur?
    - Consult notification trigger under applicable law.

1. Decision Tree: Gather the Facts

- How many individuals involved in the breach?
- Where do these individuals reside?
- Is there a forensics investigation?
  - Who is doing the investigation?
  - When will the forensics be completed?
    - Decision to notify based on facts from forensics

1. Decision Tree: Notifying Individuals

Second Step – Notifying the individual

- Who will notify the individual?
  - Contractual requirements
  - Oversight of service provider or third party

1. Decision Tree: Notifying Individuals

- Content of the notice
  - Control over content of notification (legal requirements, correct facts, etc.)
  - Template notice

1. Decision Tree: Notifying Individuals

- Delivery of the notice
  - Writing (large number)
  - Telephone (small number)
  - E-mail?

1. Decision Tree: Notifying Individuals

- Timing of the notice
  - Legal requirement
  - Contractual requirement
  - Delay in notification
    - Law enforcement investigation

1. Decision Tree: Notifying Others

Third Step: Notifying others

- Federal and state regulators
  - Notification forms
  - Talking points
- Law enforcement
- Credit reporting agencies
- Media

2. Notification Plan

- Who are the key players?
  - Incident Response Team (IRT)
    - Manage security breaches
    - All relevant facts are fed to IRT
      - Designated e-mail and telephone number
      - IRT provides facts to Legal for decisioning
      - Documents decisioning and related data obtained from key players

2. Notification Plan

- Legal
  - Privacy Counsel
    - Legal requirement to notify?
      - » Document decisioning with IRT
    - Notify regulators and/or law enforcement
      - » Consistent talking points and AG notification forms
      - » Document talking points and form with IRT
    - Contractual requirements
    - Assist with remediation efforts

2. Notification Plan

- Privacy Office
  - CPO
    - Policy considerations
      - » Notification not legally required, but notify from a policy standpoint?
      - » Document decisioning with IRT
  - Revisit data security policies

2. Notification Plan

- Public Relations
  - Consistent media script
  - Manage media
    - Blog management
      - » Different animal
- Global Security
  - Work with forensics investigation team
    - Interpret forensics report and provide facts to IRT (and Legal)
    - Document report with IRT

2. Notification Plan

- Compliance
  - Notify individuals and credit reporting agencies
    - Document with IRT
  - Assist with remediation efforts
- Information Security Office
  - Investigate root cause
  - Assist with remediation efforts
    - Document with IRT

2. Notification Plan

- Customer Service
  - Consistent telephone script
  - Keep statistics on number of customer complaints, customers satisfied, etc.
- Fraud
  - Monitor for fraud
  - Fraud attributable to a particular breach?
  - Document with IRT
- Insurance
- Outside Counsel

3. Final Thoughts

- Keep up the momentum!
  - Timing requirements
- Be careful of overly restrictive contractual requirements
  - Terms consistent with your operations?
- Ensure public message is consistent
  - Notification to individuals, telephone and media scripts, talking points and AG notification forms
- Identify root cause and remediate
  - Don't make the same mistake
- Document your actions
  - Keep IRT in the loop
- Most importantly, remain calm!

HIPAA Breach Notification Rule

- "HITECH" stands for **H**ealth **I**nformation **T**echnology for **E**conomic and **C**linical **H**ealth

- HITECH Act is part of the American Recovery and Reinvestment Act of 2009 (the stimulus legislation) adopted in February 2009

HIPAA Breach Notification Rule

- HITECH Act expanded the reach of HIPAA, which governs the privacy and security of protected health information (PHI)
- Prior to the HITECH Act, only Covered Entities were subject to HIPAA
- Business Associates (and possibly their subcontractors) are now also directly subject to many portions of HIPAA

HIPAA Breach Notification Rule

- The HITECH Act also includes new breach notification requirements
- As required by the HITECH Act, HHS issued an interim final rule for breach notification in August 2009

HIPAA Breach Notification Rule

- In the case of a Breach of "Unsecured PHI" (which has been defined by guidance from HHS), a Covered Entity must notify individuals and the Secretary of HHS of a Breach
- They must also notify the media in some cases
- A Business Associate must notify a Covered Entity of any Breach of "Unsecured PHI" that was received from or on behalf of the Covered Entity

HIPAA Breach Notification Rule

- What is a Breach?

- An impermissible use or disclosure under the HIPAA Privacy Rule that compromises the security or privacy of the PHI such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual

HIPAA Breach Notification Rule

Exceptions:

- Unintentional acquisition, access, or use of PHI by a workforce member acting under the authority of a Covered Entity or Business Associate
- Inadvertent disclosure of PHI from a person authorized to access PHI at a Covered Entity or Business Associate to another person authorized to access PHI at the Covered Entity or Business Associate
- If the Covered Entity or Business Associate has a good faith belief that the unauthorized individual to whom the impermissible disclosure was made would not have been able to retain the information

HIPAA Breach Notification Rule

- Covered Entities must notify individuals, the media (in some cases), and the Secretary of HHS of a Breach
  - Notification to Individuals
    - Notify "without unreasonable delay" and in no case less than 60 days after Breach is discovered
    - Notice must include specific information
    - Notice must be provided in a specific way

HIPAA Breach Notification Rule

- Notification to Media
  - Applies when a Breach involves more than 500 residents of a state or jurisdiction
  - Again, provide “without unreasonable delay” and in no case later than 60 days after Breach is discovered
  - Must be provided to prominent media outlets serving the state or jurisdiction
  - Notice must include specific information

HIPAA Breach Notification Rule

- Notification to the Secretary of HHS
  - When a Breach involves more than 500 individuals, notify the Secretary "without unreasonable delay" and in no case later than 60 days after Breach is discovered
  - When a Breach involves 500 or fewer individuals, the notification is due to the Secretary no later than 60 days after the end of the calendar year in which the Breach occurred
  - Report via the HHS website
  - Breaches involving more than 500 individuals are posted on the HHS website

HIPAA Breach Notification Rule

- Always remember to comply with applicable state law, even if the HIPAA Breach Notification Rule applies

Association of Corporate Counsel

Thank you for attending another presentation from
ACC's Desktop Learning Webcasts

Please be sure to complete the evaluation form for this program as your comments and ideas are helpful in planning future programs.

If you have questions about this or future webcasts, please contact ACC at webcast**@acc.com**

This and other ACC webcasts have been recorded and are available, for one year after the presentation date, as archived webcasts at **http://webcasts.acc.com**.

You can also find transcripts of these programs in ACC's Virtual Library at **http://www.acc.com/search/cfm**