Cyber Attacks and Data Breaches: A Legal and Business Survival Guide

August 21, 2012

Max Bodoin, Vince Farhat, Shannon Salimone
What this Program Covers

• Overview of Cyber Attacks and Practical Responses

• Obligations Under HIPAA and the HITECH Act

• Obligations under State Notice of Security Breach Laws
Cyber Attacks & Practical Responses
The Modern Threat: Shifting Security Trends

• Common Technologies from the 1990s
• The Perimeter: Then and Now
• First Servers, Then Workstations
• The Crimeware-as-a-Service Ecosystem
  – Tools
  – Information
  – Value
• Money Mules
• Future Security Architecture Thoughts
Rapid Response Once Attack Occurs: Executing the Cyber Incident Response Plan

- Common Cyber Attack Scenarios
- Inside Jobs
- Social Engineering
- Exploitation Malware
- Extortion and Blackmail
Cyber Incident Response Plan

• Response Team
• Reporting
• Initial Response
• Investigation
• Recovery and Follow-Up
• Public Relations
• Law Enforcement
Initial Response to Cyber Attack

• Preliminary investigation to determine whether cyber attack has occurred
• Stop cyber intrusions from spreading further into company's computer systems
• Appropriately document the investigation
Internal Investigation

• Formal investigation depending on level of intrusion and impact on critical business functions
• Gain a better understanding of the intrusion
• Increase chances of identifying attacker
• Detect previously-unknown security vulnerabilities
• Identify required improvements to computer systems
• If response team and/or IT department lack capacity or expertise:
  – Legal counsel
  – Cyber security consultant
Recovery and Follow-Up After Cyber Attack

• Cyber Incident Response Plan should address recovery of company’s computer systems by both:
  – Eliminating vulnerabilities exploited by attacker
  – Bringing the required systems back online
• Once systems are restored, the response team should:
  – Determine what cyber security management improvements are needed to prevent similar attacks from re-occurring
  – Evaluate how the response team executed the response plan
  – Consider whether the response plan can be improved
Overview of Remedies for Cyber Attacks

• Computer Fraud and Abuse Act (CFAA)
  – Principal federal statute regulating hacking and other computer crimes
  – Criminal penalties
  – Authorizes civil actions for damages and injunctive relief
  – CFAA covered in more detail in next presentation

• Other Federal Statutes:
  – Wiretap Act & Electronic Communications Privacy Act
  – Stored Communications Act
  – Trade Secret Theft, and Copyright & Trademark Infringement
Overview of Remedies, continued

- **State Computer Crime Laws**
  - Criminal and civil actions may be brought under various state laws targeting computer fraud
  - Examples:
    - California Penal Code § 502
    - Michigan Compiled Laws § 752.795

- **“John Doe” Lawsuits**
  - Tool to learn identity of hacker
  - Company has IP address of the hacker
  - Action filed in order to get discovery from ISP
Other Actions Companies Can Take to Deter or Mitigate Cyber Attacks

• Cease and Desist Letters
  – Where ongoing violations, company can send cease and desist letter before commencing a civil action

• DMCA Takedown Notices
  – Hackers sometimes post materials on third party websites or their own websites that infringe copyright
  – ISPs seeking DMCA “safe harbor” for infringing acts by their third party users must remove copyright infringing materials from user’s websites on notice

• Cyber Liability Insurance Policies
Other Issues

• Jurisdiction
  – Comes into play when deciding which law enforcement agency to contact and/or which court to file action, and applicable data breach laws
  – Consider the location of the company, the company’s servers and assets, and the attacker
  – E.g., a company based in one state may have a server located in a second state that is attacked from a system in a third state, which is being used remotely by an attacker in a fourth state

• Computation of Damages
  – Response costs including reputational harm
  – Possible third-party liability
Data Breach Notification Statutes

• Over 500 million records of individuals have been compromised in hundreds of reported data breaches since 2005

• Costs of data breaches can be significant:
  – Response costs
  – Lost business and goodwill
  – Exposure to government fines and private lawsuits

• Companies should develop Data Breach Response Plans as part of their overall compliance programs
Federal Data Breach Statutes

• There is no single federal data breach notification law that preempts the various state laws

• Federal law includes certain industry-specific breach notification laws:
  – HITECH Act enacted as part of 2009 stimulus bill amended HIPAA
  – HHS and FTC issued rules for HIPAA-covered entities and also for vendors of personal health records
  – 1999 Financial Services Modernization Act (Gramm-Leach-Bliley Act)
  – Regulates privacy and data security practices of financial institutions
  – 2007 amendments to Federal Communications Act
HIPAA & the HITECH Act
HIPAA and the HITECH Act

• Health care providers under attack:
  • In June of 2012, hackers accessed the computer network of a group of surgeons in Illinois. They infiltrated a server containing emails and electronic medical records.
  • The hackers encrypted the data and demanded payment for the password.
HIPAA and the HITECH Act

- 42 USC 17921, 17932 (breaches by covered entities and business associates)
- 42 USC 17932, 17954 (temporary breach notification requirements for vendors of personal health records, entities that offer products or services through the website of PHR vendors, entities that access information in a PHR, and third party service providers of PHR vendors)
Definition of “breach”

• “Breach” is the “unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

• A number of things are not “breaches” under HITECH
What is not a “breach”

• Any unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of a covered entity or business associate if:
  – The person is acting in good faith and within the scope of the employment or other professional relationship and
  – The information is not further acquired, accessed, used, or disclosed by any person

• But wait, there’s more! . . .
What is not a “breach” (continued) . . .

• A breach does not include inadvertent disclosures from an authorized individual at a facility to another similarly situated individual at the same facility; and

• Any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person.
• A limited data set that does not include date of birth or zip code

• Inadvertent disclosures within a covered entity or business associate, and the information is not further used or disclosed impermissibly

• Something that does not pose a “significant risk of financial, reputational, or other harm to the individual”
Harm analysis

• Perform a risk assessment to determine if there is a risk of harm to the individual (e.g. What was disclosed? Who received it? Was there sufficient mitigation? Was the stolen laptop recovered and never turned on?)

• Guidance:
  – OMB Memorandum M-07-16
  – North Carolina Healthcare Information & Communications Alliance, Inc. HITECH Act Breach Notification Risk Assessment Tool (June 2010, nchica.org)

• Document your harm analysis
Breach notifications

- 42 USC 17932: Covered entities that discover a breach must notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of the breach.

- A business associate that discovers a breach must notify the covered entity.
When is a breach discovered?

• The first day on which the breach is known, or should have been known, to any person within the covered entity or business associate (except the individual who actually committed the breach)
Deadlines for notification

• Without unreasonable delay
• No later than 60 calendar days after discovery by the covered entity or business associate
• May be delayed if law enforcement determines that notice would impede a criminal investigation or damage national security
Methods of notification

• Written notice by first class mail to the individual (or by email, if the individual has specified a preference for that communication)

• Can be done in multiple mailings as information becomes available

• If contact information for 10 or more individuals is missing or insufficient, the covered entity involved must post a conspicuous notice on its website or provide notice in major print or broadcast media in the geographic area where the individuals likely reside

• Must include a toll-free number to call for more information

• Telephone notice may be provided in addition, if matter is urgent
Content of notification

- Brief description of what happened, including the date of breach and date of discovery
- Types of unsecured protected health information involved
- Steps individuals should take to protect themselves from harm
- What the covered entity is doing to investigate the breach, mitigate loss, and protect against further breaches
- Contact procedures, including a phone number, email address, website, or postal address
Alert the media?

- If breach involves more than 500 residents of a state or jurisdiction, you must notify “prominent media outlets” serving that area.
Wall of shame

• Covered entity must notify the Secretary of HHS immediately if the breach involves 500 or more individuals, and the secretary will post a list of those entities on this website:

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html
Breach notification details

• Breaches involving less than 500 individuals must be reported to HHS no later than 60 days after the end of each calendar year

• OCR Presentation to Hospital Council of Western Pennsylvania (June 21, 2012): From September 2009 to May 2012, there were 435 reports of breaches involving over 500 individuals. Most were caused by theft and loss. Portable devices were involved 38 percent of the time.

• There were over 57,000 reports of breaches involving less than 500 individuals

• Hacking or IT incidents were involved 7 percent of the time

• May open the door to enforcement actions
State Notice of Security Breach Laws
Goals and Structure

- State Framework
- Protect Against Identity Theft
- Subject Matter
- Covered Entities
- Covered Data Subjects
- Obligations
State Framework

• State Law Governs Notification:
  – Alabama
  – Kentucky
  – New Mexico
  – South Dakota
  – Federal?
Identity Theft (1 of 2)

**Time₁**

- Creditor
- Buyer
- Credentials
- Goods or Services

**Time₂**

- Creditor
- Buyer
- Invoice
- $$
Identity Theft (2 of 2)

Time\textsubscript{1}

\begin{align*}
\text{Creditor} & \quad \text{“Credentials”} \quad \text{Imposter} \\
\text{Goods or Services} &
\end{align*}

Time\textsubscript{2}

\begin{align*}
\text{Creditor} & \quad \text{Invoice} \quad \text{Buyer} \\
\text{??} &
\end{align*}
Subject Matter: Personal Information (Typical)

- Resident’s name
- Social Security Number
- or
- Driver’s license number or state-issued identification card number
- or
- Financial account number, credit card number or debit card number
Covered Entities and Data Subjects

• Notice of Security Breach Laws Apply to Entities that:
  – Own
  – License
  – Maintain

• State Interest in Residents
Covered Entity Obligations

• **Investigation & Timing**
• **Notice**
  – Data Subjects
  – Regulators
  – Credit Reporting Agencies
• **Remedial Measures**
• **Reactive v. Proactive**
Covered Entity Considerations

• Law Enforcement
• Contractual Obligations
• Insurance
• Credit Monitoring Services
• Internal Policies and Procedures
State Law Trends

• Proactive v. Reactive
• Safeguards to Protect Personal Information
• Common Threads to Notice of Security Breach Laws
• Massachusetts
Contact Information

Vince Farhat
Vince.farhat@hklaw.com
(213) 896-2569

Shannon Hartsfield Salimone
Shannon.salimone@hklaw.com
(850) 425-5642

Maximillian Bodoin
Max.bodoin@hklaw.com
(617) 573-5819