HIPAA Summit VII
HIPAA Security Roundtable

Richard D. Marks

Davis Wright Tremaine LLP

Washington, D.C.

Seattle, Portland, San Francisco, Los Angeles, Anchorage, New York

(202) 508-6611

richardmarks@dwt.com

Aim: Corporate Compliance Plan for Information Security

Risk Analysis > Threat Model

Response Model Aligned with Business Goals & Obligations

There Are Threats

- Hackers & Crackers
- Hacktavists
- Industrial/Corporate Spies
- Trusted Insiders
  - Employees
  - Consultants
- Organized Crime
- Terrorists

Hypothetical for Analysis

- University of Washington facts
  - 4,000 complete records hacked
  - Hacker: I did it just to show you how bad your security is - a warning
- Suppose a hacker attacks your facility and posts 4,000 records to the Internet
  - What's the liability?
  - How could you have limited exposure?
  - How do you defend?
  - How do you mitigate?

What Will Plaintiffs Argue?

- Virus ex machina = res ipsa loquitur
  - (2003 Stan Tech. L. Rev. 1, 2003)
- Strict liability
  - "Ensure"
  - "Protect against *any*" threat, hazard, unauthorized use or disclosure
  - "Exceptionally high goal" for security
  - "Best of its ability"
  - " Must adjust its information security program in light of changes in technology, the sensitivity of customer information, the licensee's own changing business arrangements, outsourcing arrangements, and external threats."
- Sarbanes-Oxley (or common-law equivalent): they didn't disclose their vulnerabilities!

What Does the Lawyer Want to Tell Judge and Jury?

- The hospital had a comprehensive, coherent security plan
  - Plan complies with federal and state law
  - We were serious about it – we really followed it
  - What we planned, and what we did, created a feasible level of security considering
    - The threats we face
    - The services we furnish
    - Our financial and budgetary situation
    - The technology available in the real world
- Our plan, and how we carried it out, meets the standard required by federal and state law

"Effective program to prevent and detect violations of law"

- ✓ Establish compliance standards
- ✓ High-level personnel must have been assigned overall responsibility
- ✓ Due care not to delegate substantial discretionary authority to those with propensity for illegal activity
- ✓ Effective communication of standards
- ✓ Reasonable steps to achieve compliance with standards
- ✓ Standards consistently enforced through appropriate disciplinary mechanisms
- ✓ All reasonable steps to respond once an offense is detected (including preventing further similar offenses)
- ⌗ Same principles as Business Judgment Rule (insulating corporate officers and directors from personal liability)

What Are the Keys in Court?

- There is documentation of board participation
  - This is not a resolution saying, "we will comply with the law."
  - It is a record of board involvement in oversight of
    - Creating the "effective program"
    - Monitoring the "effective program" through its iterations
- NIST 800 Series as the model for, or a major input to, design of the effective program
- Integration of risk analysis and effective risk management in the System Development Life Cycle (SDLC) of all systems that incorporate technology (not just computer systems – business processes too)
- Incident response – and all that it implicates (acid test)

"Effective program to prevent and detect violations of law"

- The "applicable industry practice or the standards called for by any applicable government regulation" guide an organization in implementing an effective compliance program.

- Question: What are the industry's statutory or regulatory mandates?

HIPAA - Statutory Standard

"Each [covered entity] … who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards --

(A) to *ensure* the *integrity and confidentiality* of the information; and

(B) to protect against *any* reasonably anticipated

(i) threats or hazards to the *security or integrity* of the information; and

(ii) unauthorized uses or disclosures of the information; and

(C) *otherwise to ensure* compliance with this part by the officers and employees of such person."

(42 USC §1320d-2(d)(2); in effect now - does not require final security or privacy rules to become effective)

HIPAA Security Standards

- "Ensure" – Congress' intent "was to set ***an exceptionally high goal*** for the security of electronic health information."
- "No such thing as a totally secure system that carries no risks to security."
- Some trade-offs necessary – "ensuring" does not mean providing protection, no matter how expensive.
- CE takes steps "to the best of its ability"
- Balance: "identifiable risks and vulnerabilities" versus cost of various protective measures (also depends on CE's size, complexity, & capabilities)

A Litigator's View of "Best" Practices

- In security field, "best practices" are at NSA, CIA, etc.
- In commercial security field, "best" practices are at banks and other financial institutions, or in defense industry
- Health care prevailing industry practices
  - Not "best"
  - Superseded by HIPAA statute and regs
- Consider "appropriate" or "recommended" practices
- Don't make your expert vulnerable

OHCA Security Issues

- Provider OHCAs – implicit or explicit "holding out" to the public
- Security Responsibilities
  - Comprehensive and coherent security
  - Shared/ interfaced systems
    - SDLC both real & documented?
    - Security controls?
- Where are the vulnerabilities? Backdoors?
- Where are the responsibilities/ liabilities?
  - Allocation under a HIPAA compliance agreement?
  - Treatment in vendor contracts?

Security Breaches

THE WALL STREET JOURNAL.

2.
7.

MARKETPLACE

Advertising: *Mattel's Barbie brand wants to start targeting mothers* **Page B8.**

Career Journal: *Some online job sites try offering sweepstakes* **Page B16.**

redit-Card Scams Bedevil E-Stores

No Signatures to Prove ho Placed Orders, Sites re Left Footing the Bills

By Julia Angwin
Reporter of The Wall Street Journal

SEEMED LIKE a valid order. A cus-ner calling herself Amina Hadir vis-d Victor Stein's Web site in April and dered a $700 collector's edition of The liard Encyclopedia, which Mr. Stein re-thered.

e the transaction was authorized by lr. Stein shipped the book to an address occo provided by the customer and t no more about it. After all, says the rk sugar broker who writes about bil-n the side, 25% of his sales come from billiard enthusiasts.

two months later, Mr. Stein found out d way that credit-card fraud is a grow-blem for Internet merchants. Accord-ank documents provided by Mr. Stein, dir claimed to Visa a few weeks later e hadn't ordered the book. She also d a number of other items on her bill d been ordered from other Web sites, g Amazon.com. So at the request of dir's credit-card issuer, Mr. Stein's Chase Manhattan Corp., took the out of his account to reimburse the Credit Commercial de France, for its t to Mr. Stein.

er mind that Visa had authorized the ard transaction or that Mr. Stein could

A Stolen Laptop Can Be Trouble If Owner Is CEO

By Nick Wingfield
Staff Reporter of The Wall Street Journal

Irwin Jacobs came face-to-face with one of the biggest security issues facing American business executives these days: What happens when a laptop chock full of business secrets gets ripped off?

Mr. Jacobs, the chief executive and founder of **Qualcomm** Inc., had his laptop stolen from a journalism conference this past weekend in Irvine, Calif. The IBM ThinkPad laptop, which he had used to give a presentation at the conference, contained megabytes of confidential corporate information dating back years, including financial data, e-mail and personal items.

The theft was a painful reminder of one of the unforeseen costs of the New Economy's most powerful tools: new portable technologies like laptop computers, hand-held electronic organizers and cellular phones. While the devices offer unprecedented flexibility to executives, they also lead to frightening lapses in information security because of the sheer volume of data that can be hauled around on them.

Basically, business data have moved from paper to digits, but many companies aren't moving as quickly to update their security measures. Laptop theft, in particular, is "a big issue—it cuts across all different types of companies," says Richard Hefferman, a security consultant with R.J. Hefferman Associates Inc. in Branford, Conn., which performs security audits and other services for large corporations.

Some firms are being careful to protect sensi-

Wireless Devices

- Extremely useful for
  - Patient care
  - Transcription
  - Order entry
  - Remote consults
  - HIPAA administrative issues
- Security issues
  - Intercepts - encryption helps a great deal
  - Lost (or stolen) on the [subway] - physical access
  - Authenticating access
- DOD/ NIST: Restrictions on wireless LANS
  - Intercepts (1,000 feet minimum)
  - No true access port authentication (IEEE 802.11/802.11b)

Security Management Process

- More than technology; integrated with technology
- Initial and on-going risk analysis – threat assessment (outside experts?)
- Enterprise security management process
  - Computer security (includes monitoring)
  - Communications security (includes monitoring)
  - Physical security: access to premises, equipment, people, data
  - Personnel security
  - Procedural (business process) security
  - A pervasive security culture – awareness & surveillance