Risk Analysis and Security Management Under HIPAA: What's Practical, Systematic, and Cost-Effective

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

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

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"

- ✓ 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)

"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

Corporate Compliance Plan for Information Security

- ✓ Information security works best when procedures are incorporated into a system.
- ✓ Technology of these systems is rapidly evolving:
  - ** Access controls
  - ** Encryption
  - ** Firewalls
  - ** Intrusion/ anomalous event detection and alerting
  - ** Immediate incident response
- ✓ Technology is 10% of security at most.

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

There Are Threats

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

Aim: Corporate Compliance Plan for Information Security

Risk Analysis > Threat Model

Response Model Aligned with Business Goals & Obligations

NIST 800 Series - The Reference of Choice

Security Standards, 68 Federal Register p. 8334 (Feb. 20, 2003)

Security Management Process (p. 8346):

- **SP 800-30, Risk Management Guide for Information Technology Systems (2002)**

Security Awareness and Training (p. 8350)

- **SP 800-16, Information Technology Security Training Requirements (1998)**

Audit Controls (p. 8335)

- **SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems (1996)**
- **SP 800-33, Underlying Technical Models for Information Technology Security (2001)**

NIST 800 Series Publications – A Sample

- ★ SP 800-30 Risk Management Guide for Information Technology Systems, January 2002
- ★ SP 800-26 Security Self-Assessment Guide for Information Technology Systems, November 2001
- ★ SP 800-31 Intrusion Detection Systems (IDS), November 2001
- ★ SP 800-33 Underlying Technical Models for Information Technology Security, December 2001
- ★ SP 800-41 Guidelines on Firewalls and Firewall Policy, January 2002
- ★ SP 800-45 Guidelines on Electronic Mail Security, September 2002
- ★ SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996
- ★ SP 800-16 Information Technology Security Training Requirements: A Role- and Performance-Based Model, April 1998

http://csrc.nist.gov/publications/nistpubs/

NIST 800 Series
Risk Assessment Methodology

Step 1.	System Characterization
Step 2.	Threat Identification
Step 3.	Vulnerability Identification
Step 4.	Control Analysis
Step 5.	Likelihood Determination
Step 6.	Impact Analysis
Step 7.	Risk Determination
Step 8.	Control Recommendations
Step 9	Results Documentation

NIST 800 Series
Risk Assessment Methodology

http://www.csrc.nist.gov/asset/

- ✓ The purpose of ASSET is to automate the completion of the questionnaire contained in NIST Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems.“
- ✓ As described in NIST Special Publication 800-26, the results of the questionnaire provide a "method of evaluating the security of a particular system or group of systems." Through interpretation of the questionnaire results, users are able to assess the information technology (IT) security posture for any number of systems within their organization and, in particular, assess the status of the organization's security program plan.

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)

Inherent Tensions in the Security Rule

- Covered entities need enforce BAC only if:
  - CE knows of
  - BA's pattern or practice = material violation
  - CE unsuccessful at getting BA to cure breach or end violation
- Security Management
  - Ps&Ps "to prevent, detect, contain, and correct security violations"
  - Incident response, access controls, integrity controls
  - Reference: NIST 800 series
  - Requires ***constant*** monitoring & coordination
  - BA must report ***all*** security incidents (attempted or successful unauthorized attacks)

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?

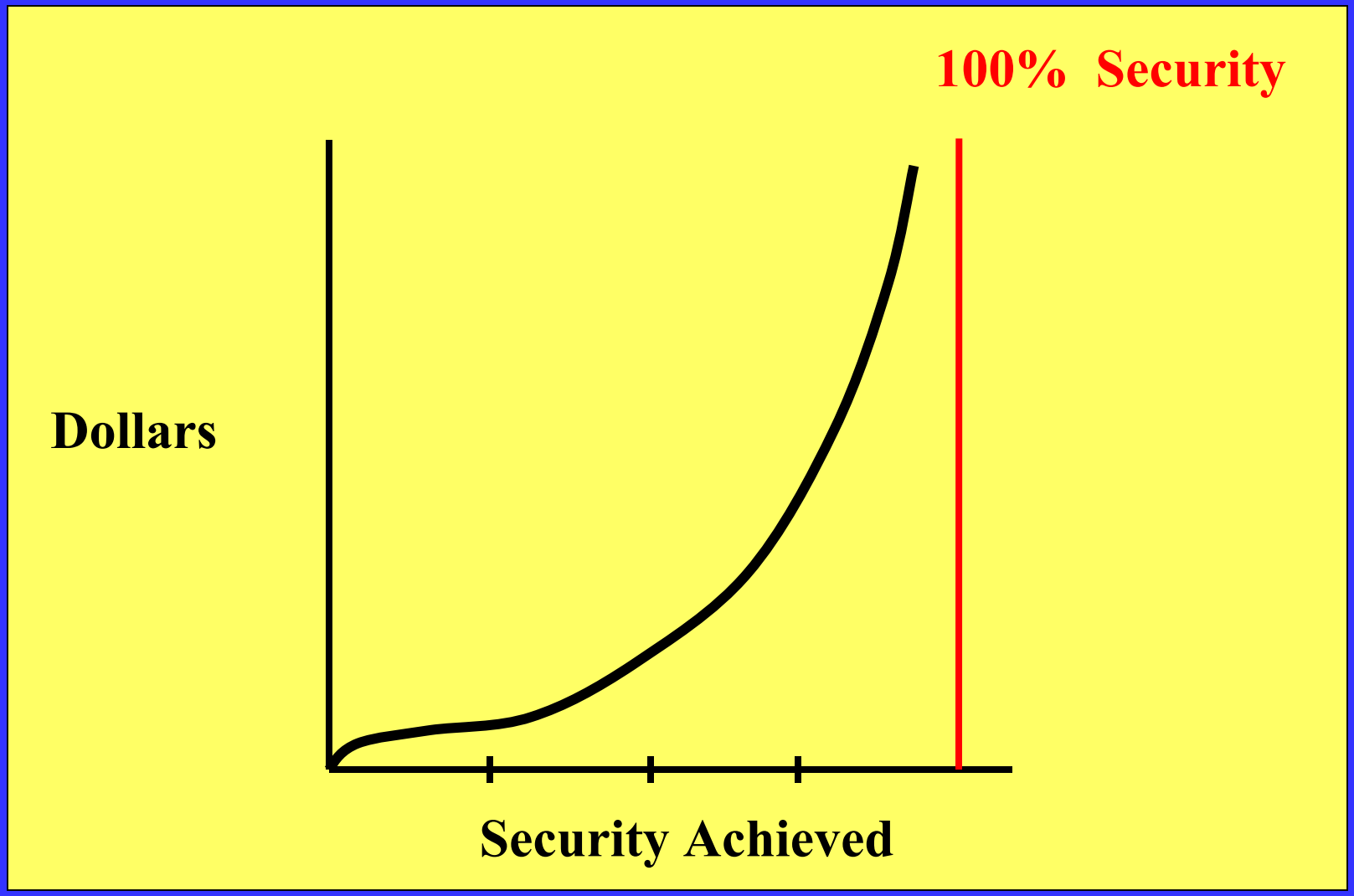
Real World of the Hospital/OHCA

- Verisign issuance of 3 spoofed certificates for use on MSN. Question: how many others?
- Same facts at a hospital/OHCA:
  - Could not trust anything on the system.
  - Safety/ malpractice concern (remember systems integration issue?)
  - Must you take the whole system down?
  - If so, how do you function? Dangers?
- What's the systems answer in managing risk?
  - Constant hot backups?
  - With ongoing integrity checking and encrypted storage?
  - Can you document precautions in SDLC?

Intrusion/Anomalous Event Detection: Incident Response – the Acid Test

- Internal Network (location of intrusion/ anomalous event detection + logging)
- Firewall
  - Proxy firewall
- Virtual Machine
- Outsourced monitoring service
- Detection is useless without the ability to analyze attack and respond very fast ("real time") and effectively
  - "Mitigate"
  - Preserve Evidence (clocks synchronized?)

Expense v. Security Achieved



NIST 800 Risk Mitigation

- ✓ When vulnerability (or flaw, weakness) exists - implement assurance techniques to reduce the likelihood of a vulnerability's being exercised.
- ✓ When a vulnerability can be exercised - apply layered protections, architectural designs, and administrative controls to minimize the risk of or prevent this occurrence.
- ✓ When the attacker's cost is less than the potential gain - apply protections to decrease an attacker's motivation by increasing the attacker's cost (e.g., use of system controls such as limiting what a system user can access and do can significantly reduce an attacker's gain).
- ✓ When loss is too great - apply design principles, architectural designs, and technical and nontechnical protections to limit the extent of the attack, thereby reducing the potential for loss.

NIST 8000 Risk Mitigation Activities

- ✓ Step 1 Prioritize Actions
- ✓ Step 2 Evaluate Recommended Control Options
- ✓ Step 3 Conduct Cost-Benefit Analysis
- ✓ Step 4 Select Controls
- ✓ Step 5 Assign Responsibility
- ✓ Step 6 Develop Safeguard Implementation Plan
- ✓ Step 7 Implement Selected Controls

Contracting For Security

General HIPAA Rule 1: When creating, moving, or storing PHI with a counterparty, the standard of care requires using a contract.

(Exception: provider-to-provider for treatment)

(Don't forget verification!)

NOTE: People will object on grounds of inconvenience, and expense (eg, we haven't used written trading partner agreements in the past)

Response: Read the statute and the rules!

Contracting for Security

General HIPAA Rule 2: When drafting a contract involving PHI, use a checklist.

- ☑ Trading partner agreement – UCC Article 4A; Federal Reserve Reg. J
- ☑ Consumer – EFTA and Regulation E (Federal Reserve)
- ☑ ESign and UETA
- ☑ Disclaim application of UCITA (MD & VA)
- ☑ Prudential considerations (e.g., state tort law + HIPAA statute; state contract law; state and federal consumer protection laws; criminal sentencing guidelines + business judgment rule)
- ☑ ERISA (e.g., health plan sponsor's monitoring duties)
- ☑ Fast-pay laws and their fraud-and-abuse consequences
- ☑ Security rules – specific requirements, prudential considerations
- ☑ TCS rules – 45 CFR § 162.915
- ☑ Security rule requirements (computer acquisitions – don't forget SDLC!)
- ☑ Privacy rule requirements

Security
When does it apply?
What's its scope?

- Wrong answer: 26 months after final security rule appears in Federal Register
- Immediate concern: 42 USC §1320d-2(d)(2) applies now to "health information"
- 45 CFR §164.530(c) requires ***appropriate*** security measures when the privacy rules are implemented on April 14, 2003 (brings application of the final security rules forward)

What's Different After Enron?

- The Sarbanes-Oxley Act of 2002, Pub. L. 107-204, 116 Stat. 745 (2002)
- Emphasis on management's responsibility "for establishing and maintaining an adequate internal control structure and procedures for financial reporting"
- Reporting obligations cover more than GAAP matters, extending to material operational issues.
- A secure information infrastructure is central to many companies' operational capabilities. Hence, the material condition of the business will be assessed, and certified by officers, in that light.

What's Different After Enron?

- Result: a new standard of care for corporate information security
  - Founded on GLB & HIPAA statutory standards
  - Reinforced by state case law and regulatory standards (GLB)
  - Formalized by Sarbanes-Oxley disclosure requirements for publicly traded companies
- Prediction: this standard of care will transfer to non-profits, then to enterprises generally

What's Different After Enron?

- 5 recent (2002) Delaware Supreme Court opinions siding with shareholders in claims against directors.
- Delaware Chief Justice Norman Veasey's comments at U. of Delaware's forum on corporate governance, Oct. 2002:

  "Directors who are supposed to be independent should have the guts to be a pain in the neck and act independently."

What's Different After Enron?

- NY Attorney General Eliot Spitzer (press release, Jan. 29, 2003), proposing to apply corporate reform provisions of Sarbanes-Oxley to nonprofit organizations, to achieve "accountability" for nonprofit entities in NY, because they "have custody of billions of dollars in charitable funds."
- U.S. Sentencing Commission's action (Jan. 10, 2003) adopting an emergency plan for harsher sentences in corporate crime cases.
- New California law (SB 1386) requiring any online business serving customers in California to notify customers of computer security breaches that reveal customers' names in association with an identifying number (*e.g.*, SSN, driver's license, credit card). (Will companies doing business in California find it necessary to notify all customers, wherever located? How does this change operations for banks and financial companies, which often do not publicize hacks?)