Cybersecurity – Don't Be Caught Unprepared

Wyatt J. Holliday, CEBS
Attorney
Shumaker, Loop & Kendrick LLP
Toledo, Ohio

International Foundation of Employee Benefit Plans
Education | Research | Leadership

Overview

- Fiduciary Obligations and Liability
- The Three-Legged Stool of Cyber Security
- Service Provider Contracts
- Cyber Liability Insurance

An Introductory Thought:

- Nothing is 100% secure
  - The FBI told congress the Sony hack would have defeated 90% of the security then in existence
  - All the security in the world can be defeated by negligence or intentional bad acts

Fiduciary Duty

- The Prudence standard
  - Prudent person
    - Procedural prudence
    - What can you prove?
  - Acting in a like capacity and familiar with such matters
    - Expertise not a requirement
    - Must know enough to know what you don’t know
  - Education!

Fiduciary Duty

- A cyber breach becomes a fiduciary breach when a prudent individual familiar with cyber security would have done something different
- So what do we do now?
  - Sound internal practices
  - Sufficient due diligence on external practices

Who Is Liable?

- In a word: Everyone
- Liability attaches to the Covered Entity, Business Associate, and The Business Associate's Business Associate
- Sanctions:
  - HIPAA
  - State Law – 47 states and D.C.
  - Civil liability – HIPAA and state law may be cited as "best practices"

Who Is Liable?

- Monetary Penalties:
  - $100 to $50,000 per violation, depending on the level of culpability
  - $1.5 million cap per calendar year for multiple violations of identical provisions
- Criminal penalties of up to 10 years' imprisonment
- Willful neglect is frowned upon.
  - Even a possibility of a violation due to willful neglect can trigger monetary penalties
- 45 CFR 160.400 *et seq*

A thought about liability:

- “Surviving” a breach can mean a lot of different things.
- How will you/your board/your fund look in the letters, press releases, and news stories?
- “We did everything we could.”

The Three-Legged Stool of Cyber Security

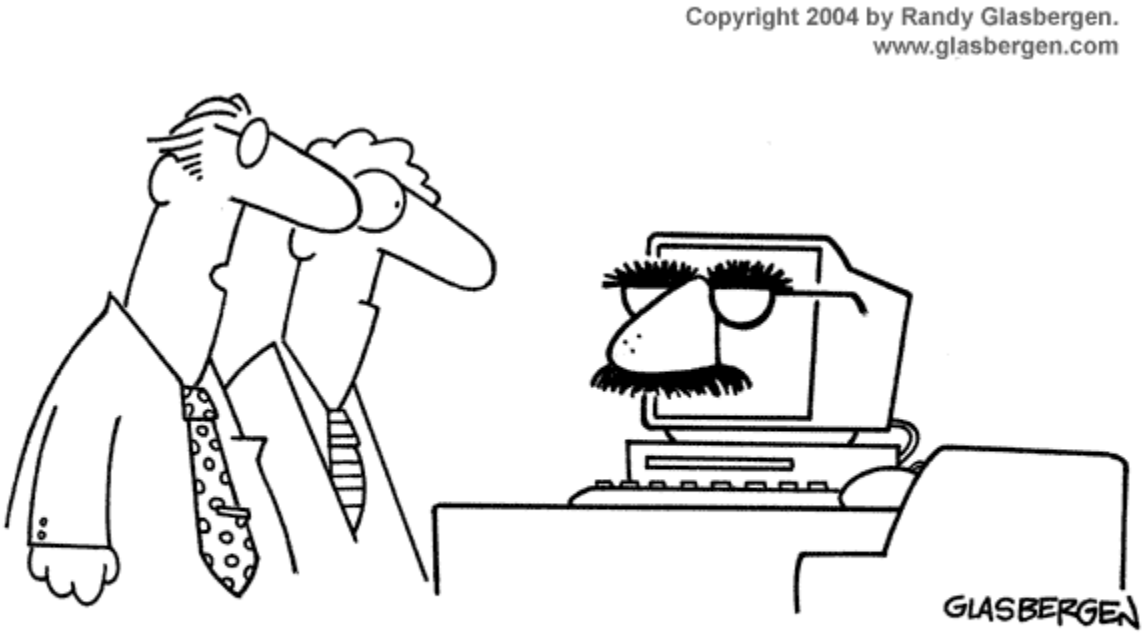
- The Things: Data Security and Management
- The Places: Physical Security
- The People: Personnel Management

- These elements must exist both in-house and at EVERY ONE of your service providers!

A Brief Interlude: Due Diligence

- We just said this a few slides ago, but it is really important.
- Boards of Trustees are (probably) not e-security experts.
- They can ask the right questions.
- Procedural Due Diligence: What can you prove?

Data Security and Management



"I'm sure there are better ways to disguise sensitive information, but we don't have a big budget."

Data Security and Management

- How is your data being managed?
  - "At rest"
  - Hard disk encryption
  - De-identification
- "In flight"
  - Encrypted connections
- HIPAA is a good starting point

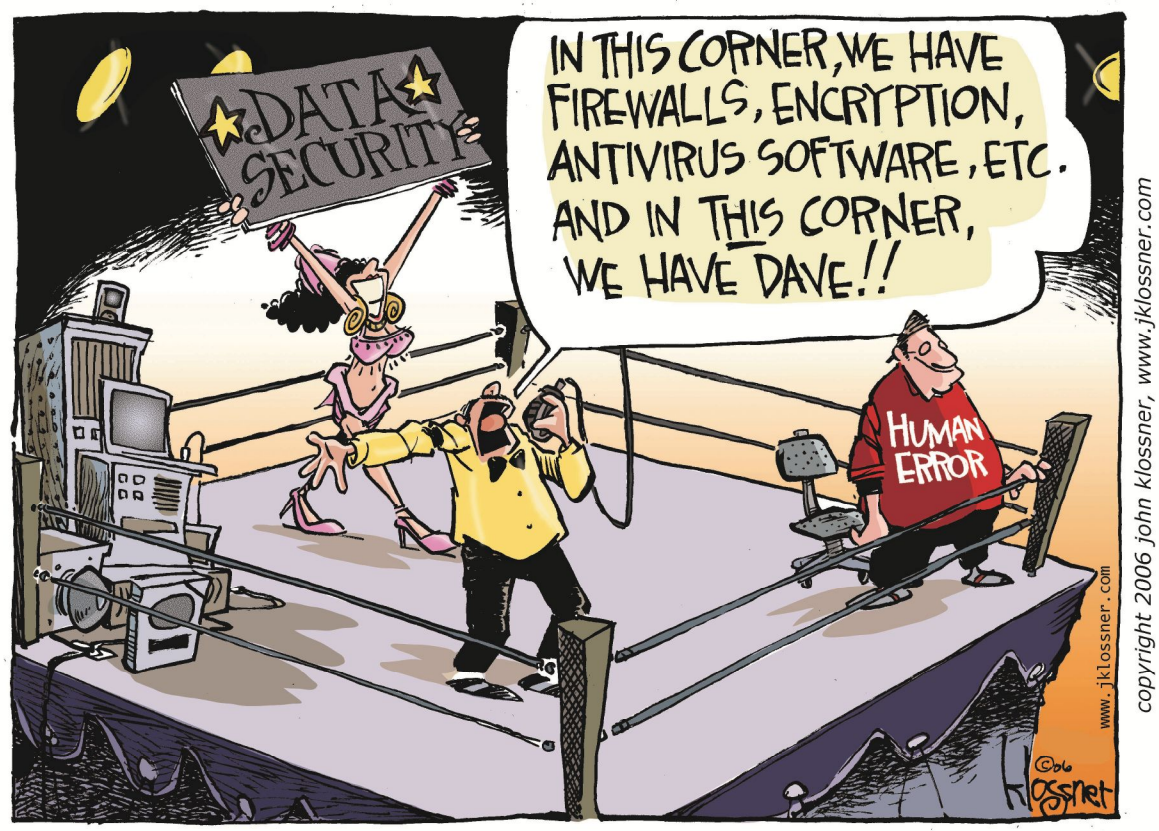
Physical Security

"I DON'T THINK YOU UNDERSTAND THE CONCEPT of CYBERSECURITY."

Physical Security

- Who can physically get to your data?
  - Fences, barriers, electronic/physical keys
- Document Disposal
  - Shredding, printer security
- Portable Devices
  - PCs, tablets, smartphones

Personnel Management



Personnel Management

- All the security in the world can be defeated by negligence or intentional bad acts.
- Computers <u>only</u> do what they're told; people often do the opposite of what they're told.

Personnel Management

- Training and Policy
  - Security training should be regular and on-going
    - Must be both for IT professionals and non-tech employees
    - Example: password strength

Personnel Management

- Internal Audit Protocols
  - Both in-house and at service providers
- How often do you
  - Review user access levels?
    - Each user should have the minimum amount of access necessary for their job.
  - Validate employee directories?
    - Written process at termination
    - Multiple points of entry

Personnel Management

- The “Squeaky Wheel” factor
- The social element of security
  - Employees are reviewed and compensated on meeting deadlines and hitting productivity goals
  - Security elements take time, energy and focus away from what employees are being measured on

Business Associate Agreements

- HITECH (2013) changed BAAs for cyber security:
  - "creates, receives, maintains or transmits" to BA description for receiving or producing data for CE
  - Any sub-BAA at least as stringent
  - BA must report breach "without unreasonable delay," but definition of that in BAA suggested.
    - Statutory 60-day limit impacts plan's ability to react appropriately.
  - If BA is performing CE's obligation under privacy rule, BAA must require that BA abide by privacy rule.

Vendor Contract Provisions

- Transfer as much liability as possible
  - Negotiating Risk Ideally, your contract will transfer any risk or fall-out from the breach
  - But there are trade-offs
    - Liability versus fees
    - Vendors may not be able to secure adequate insurance
- Require notification of a breach event ASAP and before any regulatory notifications

Vendor Contract Provisions

- DOL hot-button: Limitations of Liability
  - DOL Advisory Opinion 2002-8A
  - LoL/indemnification not *per se* imprudent or unreasonable, <u>BUT</u>
  - Provisions re: fraud/willful misconduct void as against public policy
- Provisions limiting liability or indemnifying for negligence or unintentional malpractice are ONLY reasonable if:
  - Such provisions are reasonable in context AND
  - The fiduciaries have assessed comparable services at comparable costs from alternate vendors who do not require such terms or who provide greater protection to the plan.
- The plan MUST put any such contract out to bid!

Cyberliability Insurance

- Fiduciary policies usually not sufficient.
  - Endorsements rarely cover breach notification, crisis management and response expenses
    - 1st Party Breach Response
  - Often sub-limited to fraction of the policy limit
    - 1st and 3rd Party

Cyberliability Insurance

- 1st Party Breach Response
  - Breach Response
    - Pre-claim counsel
    - Crisis management, forensics and call center
    - Notification expense including credit monitoring
  - Fines and Penalties Assessed By
    - HIPAA/HITECH
    - Payment Card Industry (credit cards, HRA cards)
    - State regulators
  - Other First-Party Insurance
    - Loss and restoration of data
    - Cyber extortion, computer fraud, funds transfer fraud

Cyberliability Insurance

- 3rd Party Breach Response
  - Legal liability and defense costs (litigation and regulatory)
  - Liability for online media activity
    - Defamation, copyright, trademark infringement
  - Judgments and settlements

Key Takeaways

- Fiduciaries MUST not only perform the diligence due, but they must be able to prove it!
  - Know what questions to ask
- Review all Business Associate Agreements and service provider contracts for proper risk-transfer, protections.
- A robust cyber liability insurance policy provides holistic, expert response.