Legal, Compliance, & Regulatory

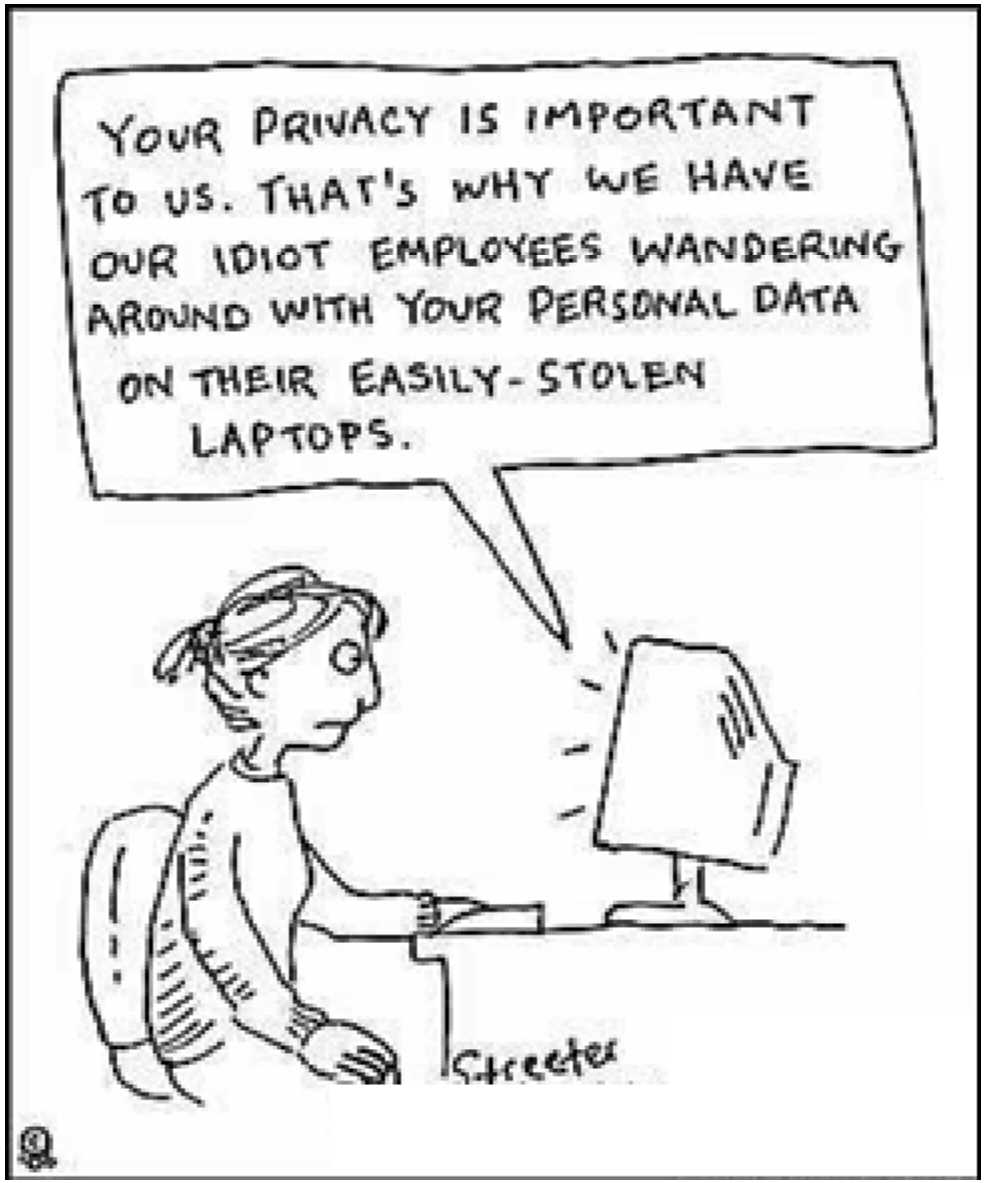
Privacy Requirements and Risks: A Proactive Approach

March 17, 2014

Angela Hoteling-Rodriguez
MedAmerica Insurance Company

Stephen Serfass
Drinker Biddle & Reath LLP

ILTCI


YOUR PRIVACY IS IMPORTANT TO US. THAT'S WHY WE HAVE OUR IDIOT EMPLOYEES WANDERING AROUND WITH YOUR PERSONAL DATA ON THEIR EASILY-STOLEN LAPTOPS.
Greeter

Agenda

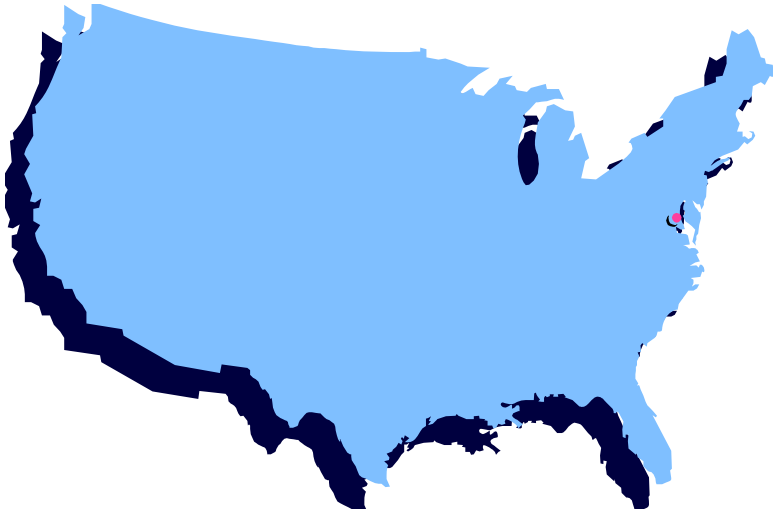
- Brief Overview of Applicable Laws, State and Federal
- Case Studies of Breaches and the Lessons Learned
- Breach Statistics: Trends and Costs
- Privacy Risk Mitigation Strategies

Legal Overview

Legal Overview

- Breaches today have implications in both state and federal law

State Law



Federal Law

Legal Overview

Several Federal Statutes Regulate Information Privacy

- Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its amending Health Information Technology for Economic and Clinical Health Act ("HITECH")
- Gramm Leach Bliley
- Other Federally based private party claims under:
  - Electronic Communications Privacy Act
  - Stored Communications Act
  - Video Privacy Protection Act
  - Driver's Privacy Protection Act

Legal Overview

What's New to HIPAA from an LTCi perspective?

- Expanded universe of Business Associates, new Business Associate Agreements required
- Elimination of Business Associate "safe harbor"
- For Hybrid Entities, more must go into the "healthcare component"
- Revised Breach protocol (guilty until proven innocent)
- Other slight tweaks (Notices of Privacy Practices must be updated, individuals have new rights, etc.)

Competing with the Federal Laws are a Myriad of State-Specific Obligations:

- 46 states have adopted security and data breach notification laws.
- All require prompt notification; some establish penalties and private rights of action.
- Statutes typically define:
  - data breach
  - types of protected information
- Some set thresholds for the notice requirement, *e.g.*, a reasonable basis to believe the breach will result in harm.

Other Features of State Statutes

- Application to data in paper form (at least 3)
- Reporting to government/media if substantial impact (think >500 people) (28)
- Safe harbor if alternate notification policy followed (34)
- Type of notice – norm: paper or electronic consistent with E-Sign requirements (with substitute notice available if expensive)
- Private right of action (11 – but most are silent)
- Penalties (36)
- There are others!

State Statutes

- **Beyond Notice** – Active security measures to prevent data breaches
  - **Conn. Gen. Stat. Ann. § 42-471**- Safeguarding of personal information. Social Security numbers. Privacy protection policy. Civil penalty.

    (a) Any person in possession of personal information of another person shall safeguard the data, computer files and documents containing the information from misuse by third parties, and shall destroy, erase or make unreadable such data, computer files and documents prior to disposal.

State Statutes

- **Beyond Notice** – Active security measures to prevent data breaches
  - **Other States**
    - **Arkansas** [ARK CODE ANN. § 4-110-104(b)];
    - **California** [CAL. CIV. CODE § 1798.81.5(b)];
    - **Maryland** [MD. CODE ANN., COM. LAW § 14-3503];
    - **Massachusetts** [MASS. GEN. LAWS ch. 93H § 2(a)];
    - **Nevada** [NEV. REV. STAT. § 603A.210];
    - **Rhode Island** [R.I. STAT. 11-49.2-2(2),(3)];
    - **Oregon** [OR. REV. STAT. § 646A.622];
    - **Texas** [TEX. BUS. & COM. CODE ANN. § 48.102(a);
    - **Utah** [UTAH CODE ANN. § 13-44-20].

State Statutes – Beyond Security Breach Notification Laws

- **Unfair and Deceptive Trade Practices Act**

  - Some variation of this type of consumer protection statute has been enacted by states

  - Typically enforced by the state's Attorney General, but some states have private rights of action

Case Studies and Lessons Learned

Case Studies and Lessons Learned

- July 2013: HHS settled with WellPoint
- An investigation determined that WellPoint did not implement “appropriate administrative and technical safeguards” for its databases, online applications and software systems

Case Studies and Lessons Learned

- As a result, the protected health information of 612,000 people was disclosed because of lax electronic access standards
- HHS and WellPoint agreed to a **$1.7 million** fine and a corrective action plan to ensure future compliance

Case Studies and Lessons Learned

- Lesson: your systems are being tested every day, be vigilant to ensure your technical protections are sufficient

Case Studies and Lessons Learned

- August 2013: HHS settled with Affinity Health Plan, Inc., a not-for-profit issuer of Medicaid managed care plans in the New York metropolitan area
- A local CBS affiliate purchased a copy machine previously leased by Affinity and found that the machine still stored the protected health information of about 344,000 people

Case Studies and Lessons Learned

- This breach led to an investigation into Affinity's past compliance history and current practices
- HHS and Affinity agreed on a **$1.2 million fine** and a corrective action plan to ensure future compliance

Affinity Health Plan
Dedicated to Excellence

Case Studies and Lessons Learned

- Lesson: Each type of technology used may present a new area of exposure

Case Studies and Lessons Learned

- Sometimes even small-scale breaches or organizations face full-blown investigations
- January 2013: HHS settled with The Hospice of North Idaho ("HONI")
- An unsecured HONI laptop, containing PHI for 441 HONI patients, was stolen
- HHS and HONI settled on a **$50,000** fine

Case Studies and Lessons Learned

- Lesson: encrypt your laptops, a stolen encrypted laptop may not constitute a breach

> "Encryption is an easy method for making lost information unusable, unreadable and undecipherable."
>
> Former OCR Director Leon Rodriguez


TARGET
COMPLAINT DEPT.
THIS CREDIT CARD DATA THEFT BRINGS NEW MEANING TO BEING A TARGET CUSTOMER!
DAVE GRANLUND © www.davegranlund.com

Case Studies and Lessons Learned

- The Target Breach, while not a HIPAA issue, still shares a lesson uniform to almost every company
- What happened?
  - When? Nov. 27, 2013-Dec. 18, 2013
  - Who? hackers stole an HVAC company's login credentials and gained remote access to Target's system, which the hacker then exploited to find credit card information
  - How? An employee at the HVAC company clicked a phishing e-mail's link
  - What? names, mailing addresses, e-mail addresses, phone numbers, and credit and debit card information of up to 70 million individuals (notably, Target was PCI DSS compliant)

Case Studies and Lessons Learned

- First Lesson: Don’t hold sensitive information unless you need it (and are allowed to have it)
- Minnesota Statute § 325E.64 subd. 2 states:
  - Businesses may not retain “the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data” of customers “subsequent to 48 hours after authorization of the transaction.”

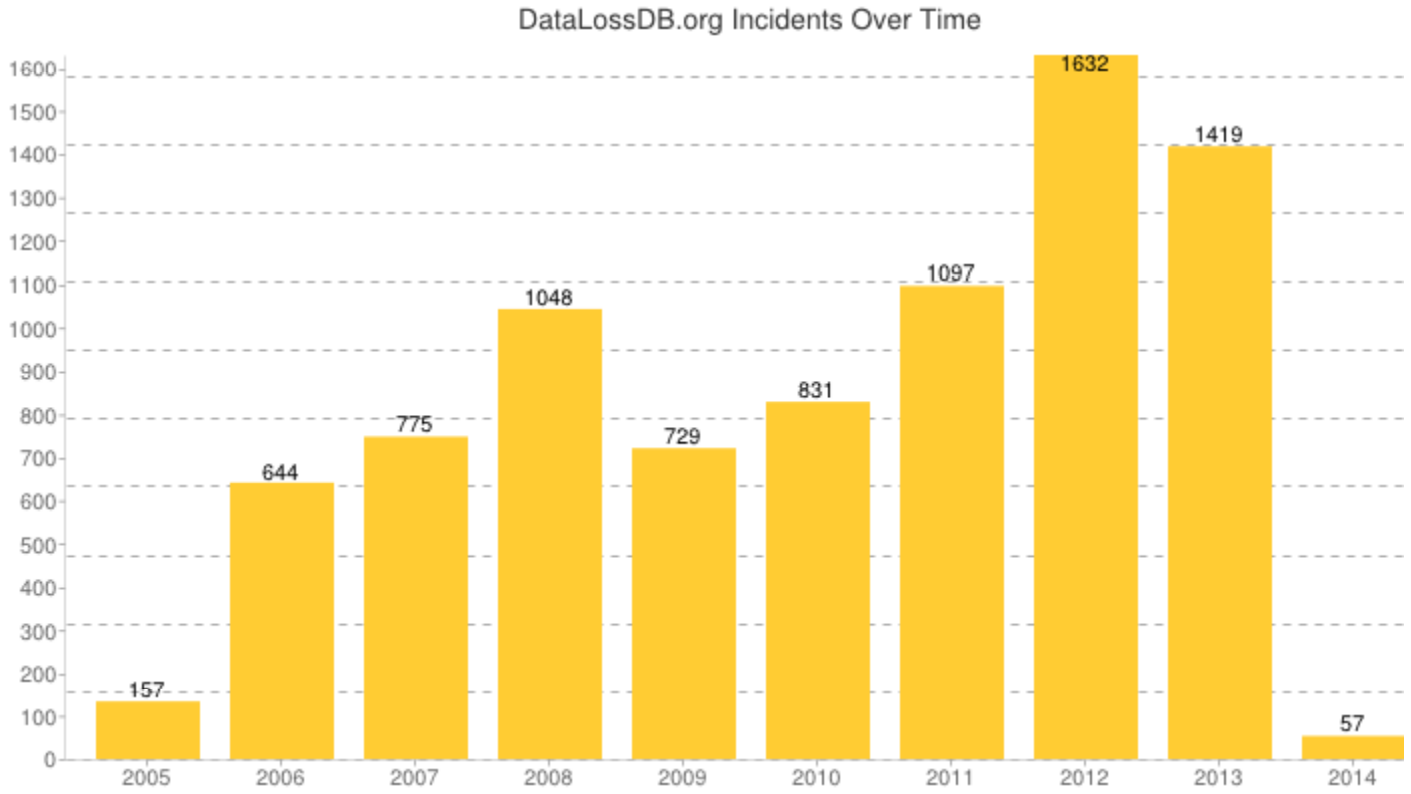
Case Studies and Lessons Learned

- Second Lesson: If a breach is big enough, everybody will come after you.
  - More than 70 class action suits brought by customers
  - Banks and Credit Cards have begun lawsuits to recover for reimbursements to customers
  - Justice Department confirmed a criminal investigation is underway
  - Three congressional committees have scheduled hearings in response to consumer outrage

- Third Lesson: Know thy Vendors
  - The HVAC vendor needed access to the remotely monitored heating and cooling information for Target locations, but somehow this access was exploited for far more
  - Obviously only engage vendors you can trust, but be mindful to only grant them the minimum access necessary to accomplish their task.

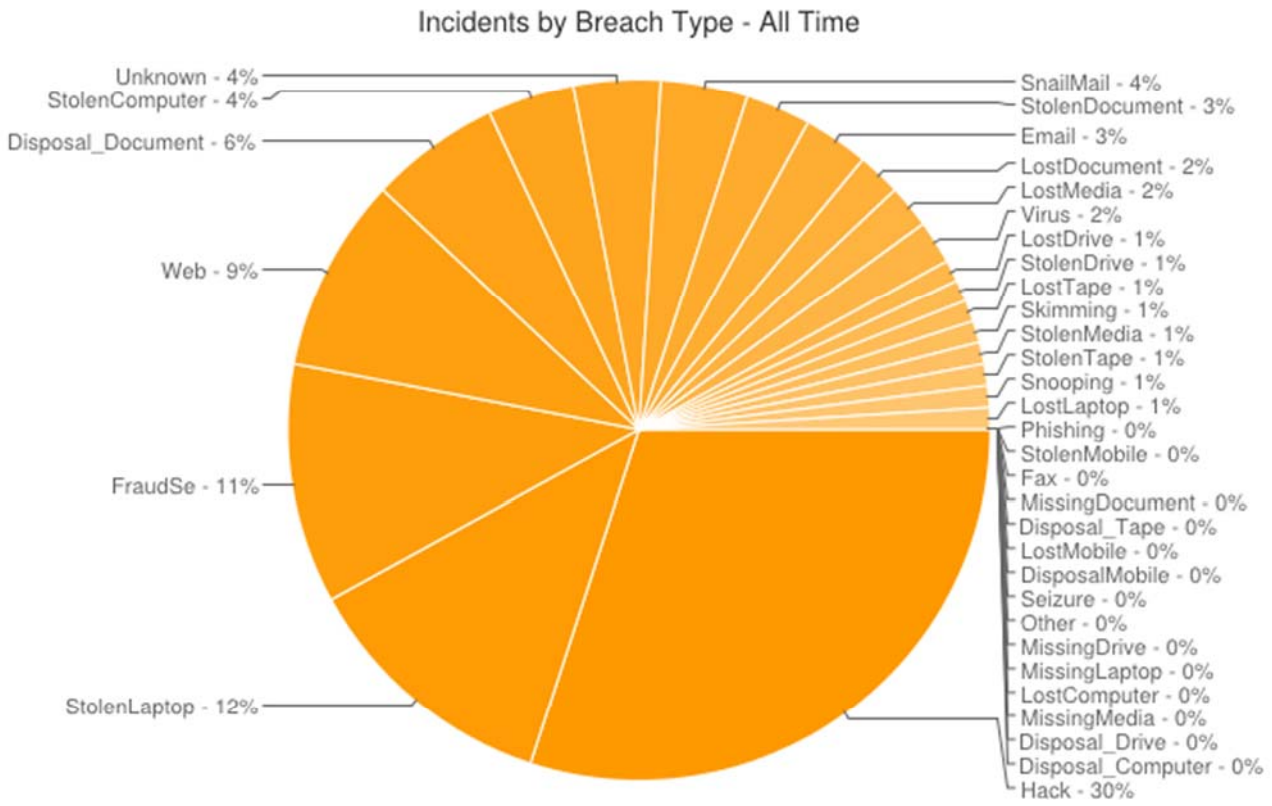
Breach Statistics: Trends and Costs

Number of Reported Data Breaches: 2005 – Present



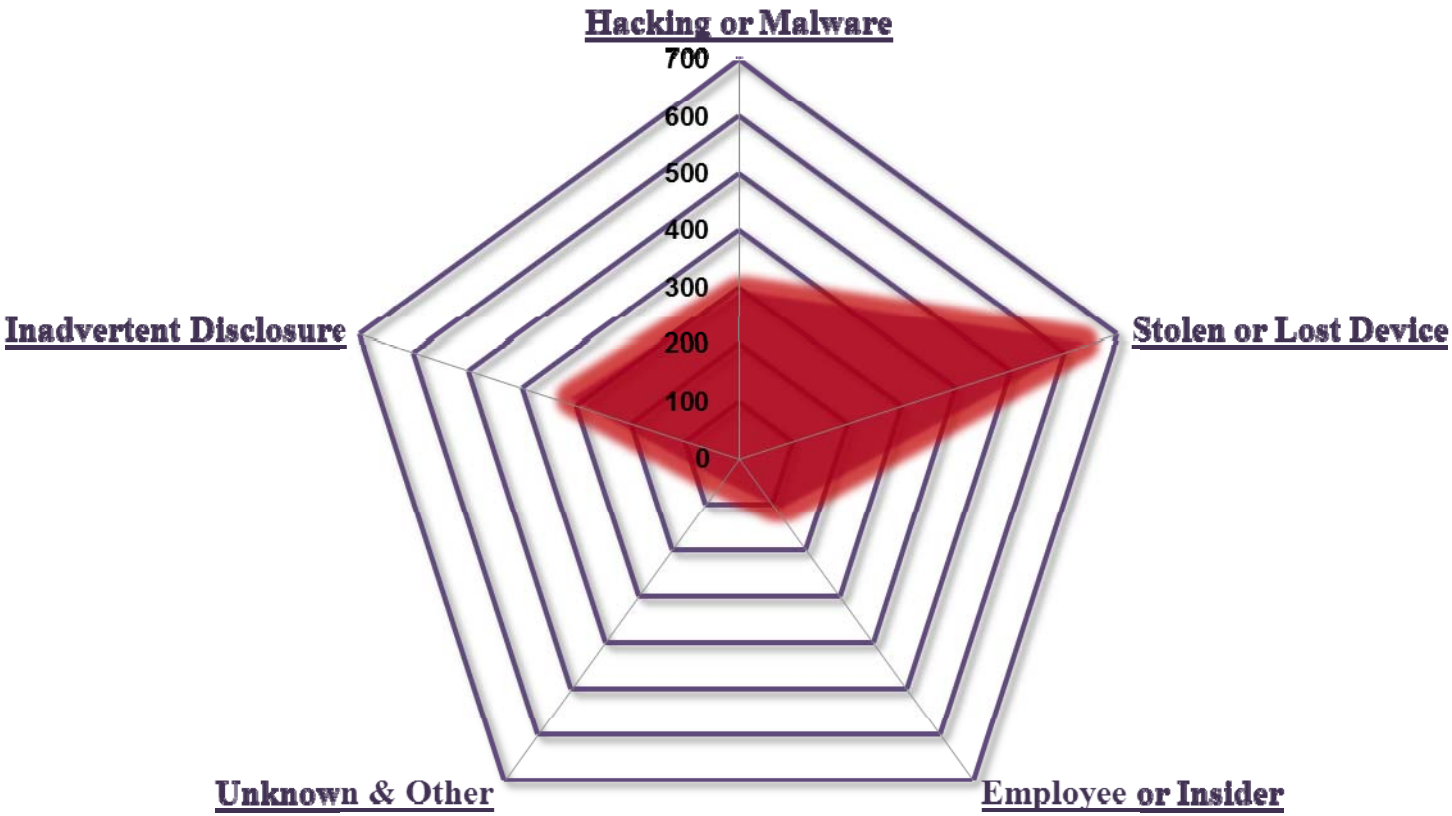
Source: DataLossDB.org
Available at: http://datalossdb.org/statistics

Incidents by Breach Type:



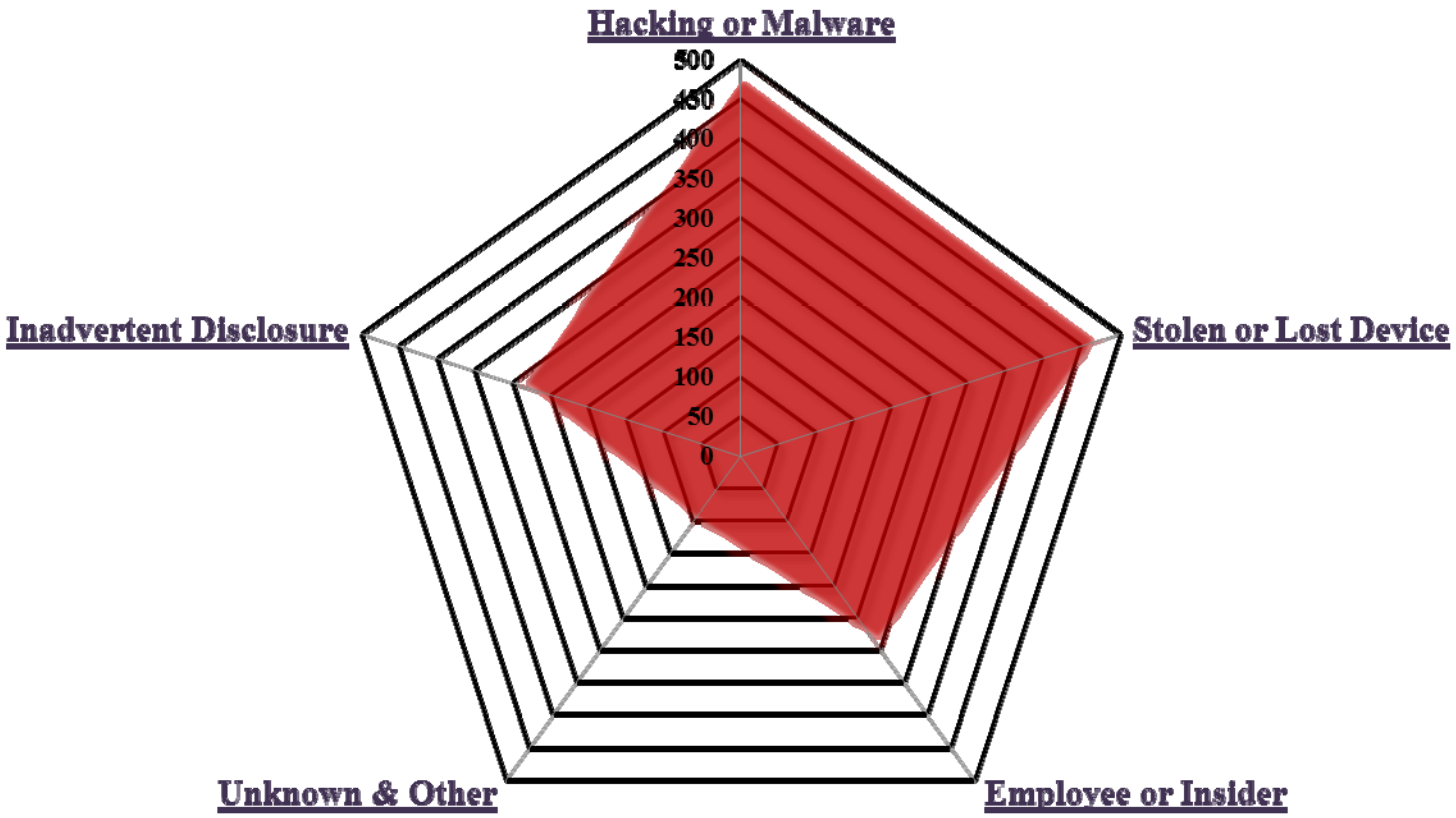
Source: DataLossDB.org
Available at: http://datalossdb.org/statistics

Electronic Data Breaches by Breach Type: 2005-2009



Source: Privacy Rights Clearinghouse
Available at http://www.privacyrights.org/data-breach

Electronic Data Breaches by Breach Type: 2010 - Present



Source: Privacy Rights Clearinghouse
Available at http://www.privacyrights.org/data-breach

Cost of a Data Breach

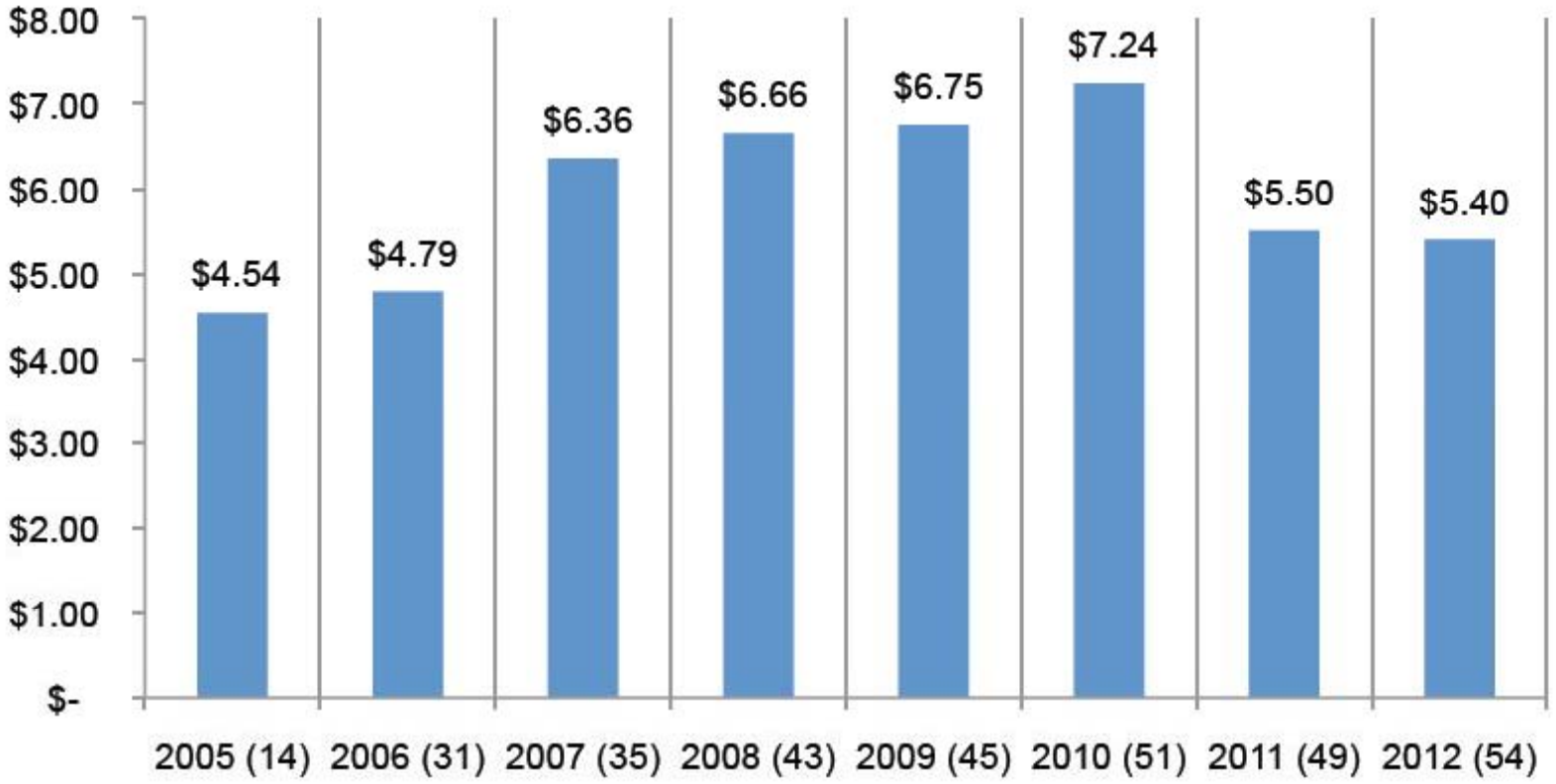
In a 2010 study, it was determined that the average organizational cost of a data breach caused by the loss of a single unencrypted laptop was **$56,165.00.**

Of 329 participating organizations, the average number of lost laptops per organization per year was **263**.

Source: Ponemon Institute, *The Billion Dollar Lost Laptop Study*, sponsored by Intel (9/30/2010); available at http://newsroom.intel.com

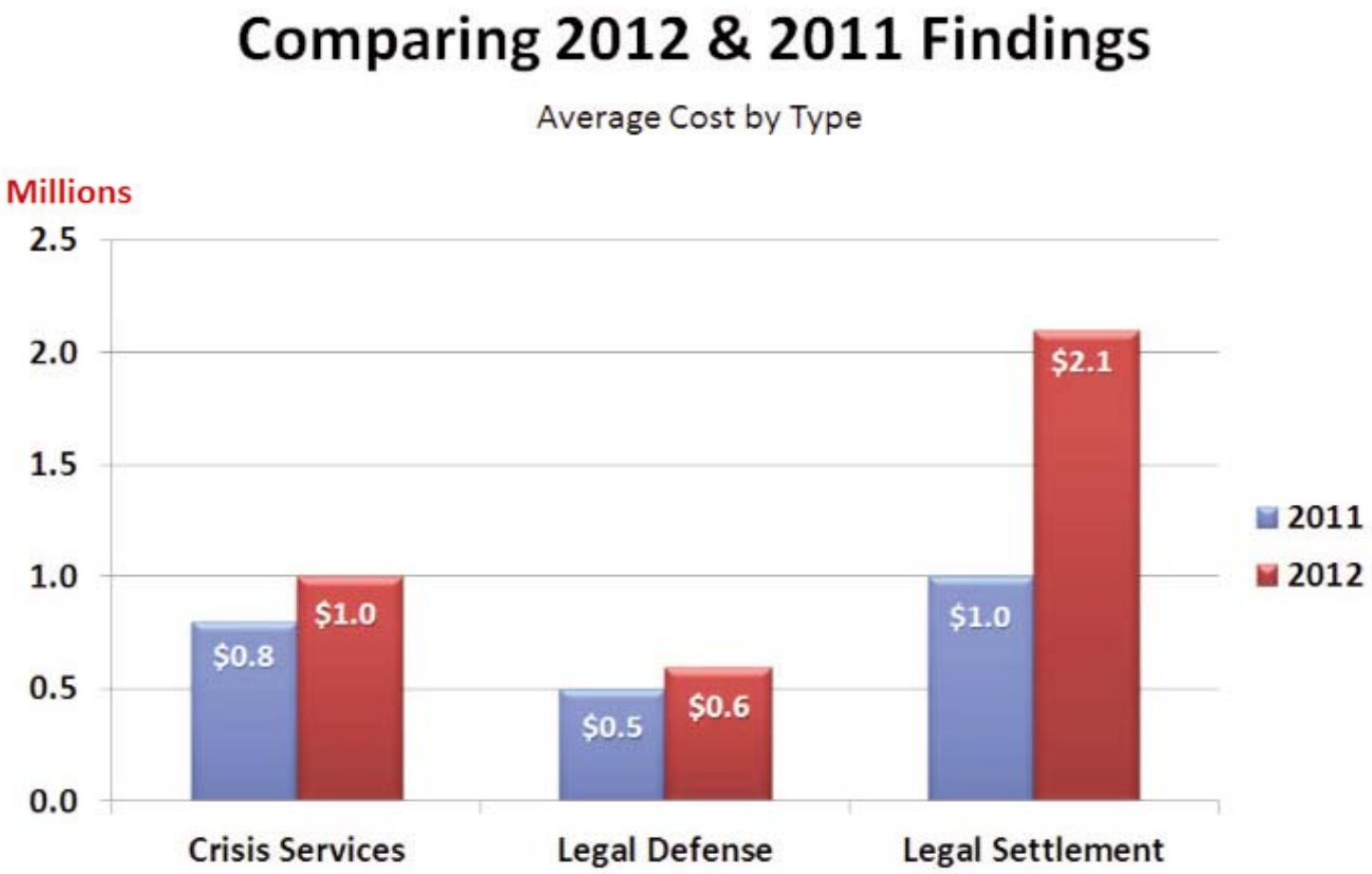
Cost of a Data Breach

Average total organization cost of a data breach
(in millions)



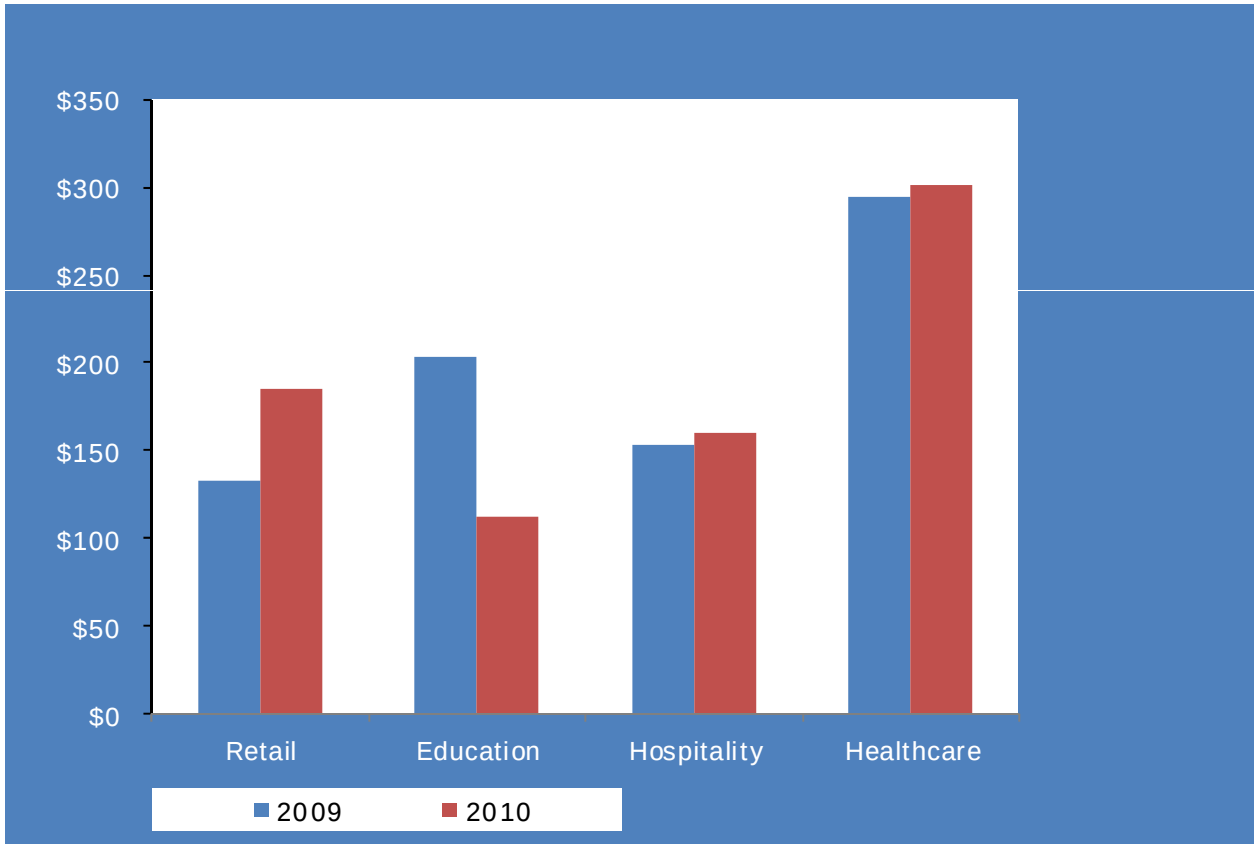
Source: Ponemon Institute, *2013 Cost of a Data Breach: United States*, sponsored by Symantec (5/2013)

Fallout From Data Breaches



Source: NetDiligence, *Cyber Liability and Data Breach Insurance Claims, (*October 2012)

Cost per record – By industry



Data Breach Response Costs:

1.Identify the Source of the Breach and Information Compromised – Forensic Experts

2.Consult Legal Experts

3.Public Relations

4.Notification

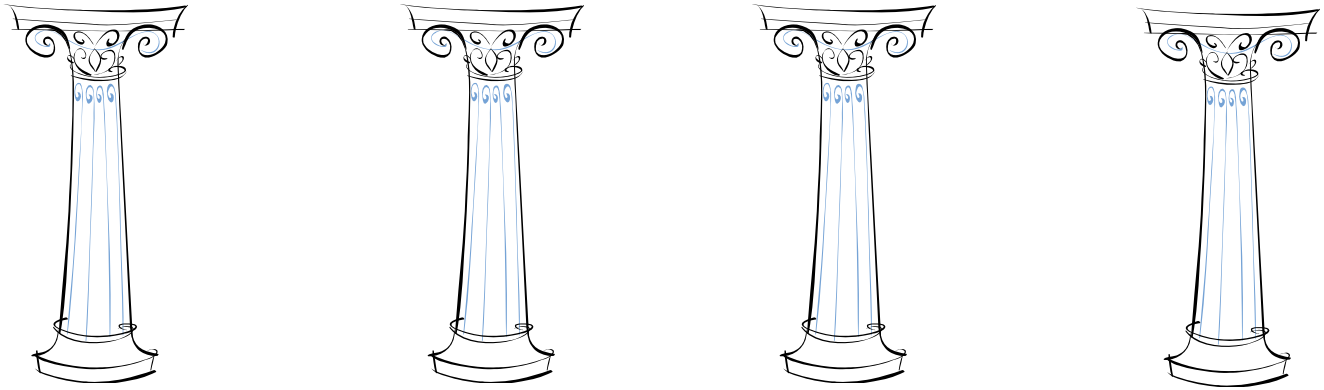
- Mandatory;
- Voluntary;
- To avoid fraud allegations.
  - In re Heartland Payment Systems Inc. Securities Litig., 2009 WL 4798148 (D.N.J. Dec. 7, 2009)

5.Provide Assistance for Affected Individuals & Entities (e.g. creditor monitoring)

Privacy Risk Mitigation Strategies

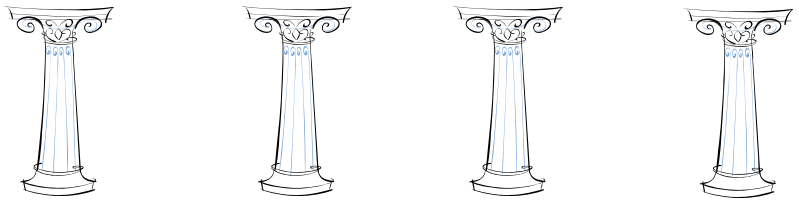
Privacy Risk Mitigation Strategies

There are Four Pillars essential to a Privacy Compliance Program

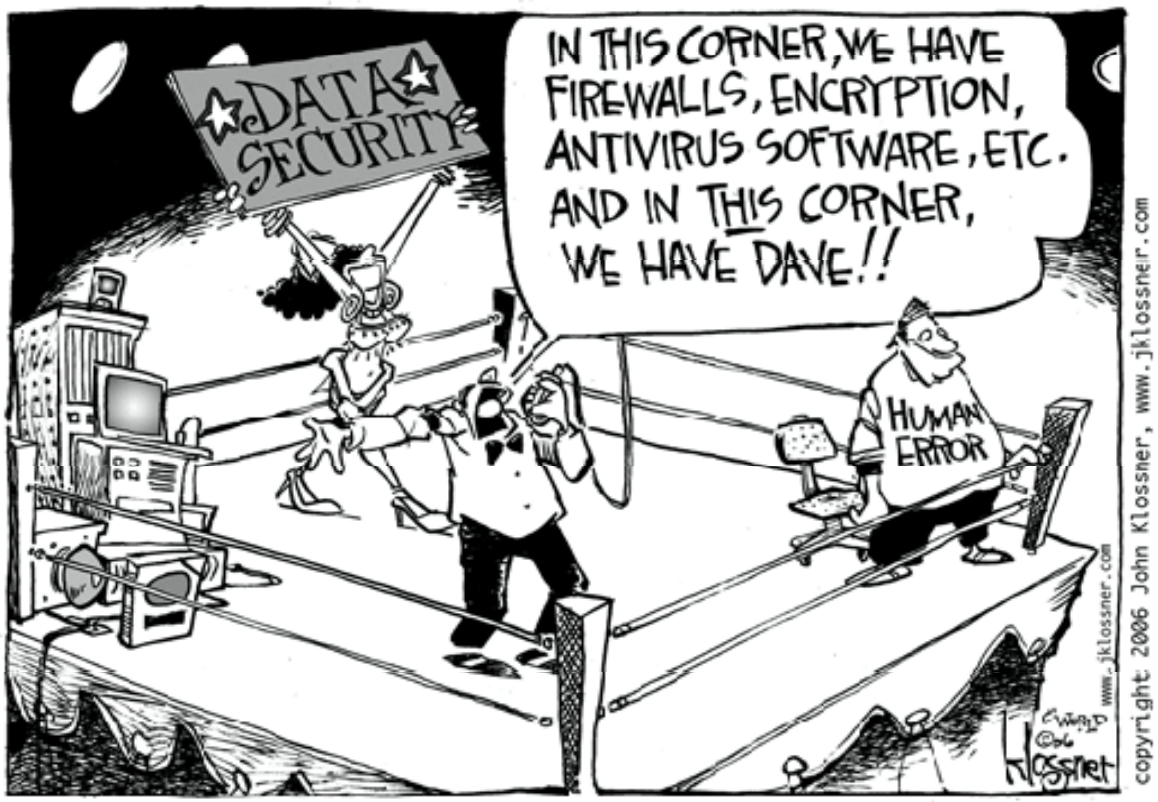


Privacy Risk Mitigation Strategies

- Pillar 1: Policies and Procedures
  - Current document retention and destruction policy
  - Procedures implementing destruction aspects of above policy (electronic and paper)
  - Notice of Privacy Practices

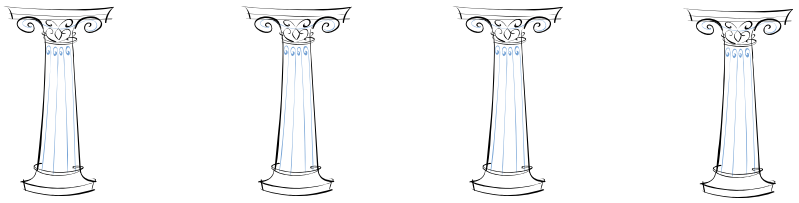


People


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
copyright 2006 John Klossner, www.jklossner.com
www.jklossner.com
Klossner

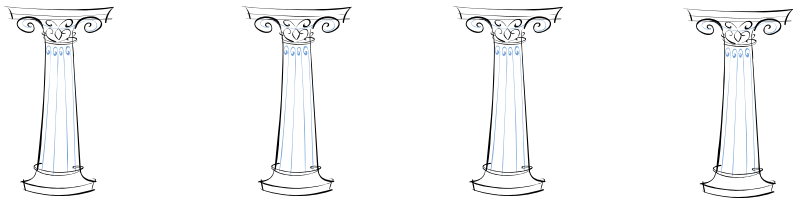
Privacy Risk Mitigation Strategies

- Pillar 2: Staff Training & Education
  - Code of Conduct
  - Mandatory employee training program
    - On-boarding
    - Routine/Annual
    - Ad Hoc (in response to trends or incidents)
    - Varied Media (on-line, video, posters, etc.)
  - Evidence of employee training/communications



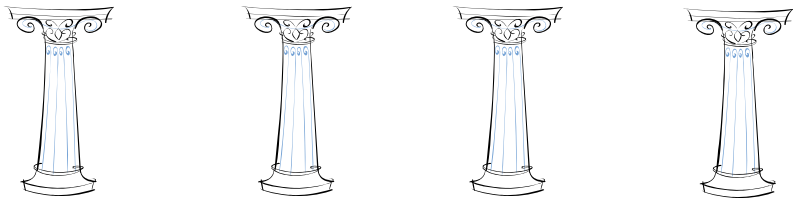
Privacy Risk Mitigation Strategies

- Pillar 3: Risk Identification & Mitigation
  - Written policies and procedures paired with audit/quality assurance reviews (internal vs. external)
    - *E.g.* Minimum necessary access paired with systematic controls and routine access audits
  - Accounting of Disclosures system, paired with a Breach Notification process
    - *E.g.* Risk Analysis document for each incident "feeding" breach notification



Privacy Risk Mitigation Strategies

- Pillar 4: Business Associates
  - Business Associate Agreements (revision required by Omnibus)
  - Communication of enhanced expectations (given expanded obligations under Omnibus)
  - Audit/Quality Assurance Review



Consider Cyber Liability Insurance

- Estimates of the value of the standalone cyber market in the US vary between $400 million and $800m (some is still bundled with E&O coverage)
- Some carriers have seen demand surge by 270% between 2009 and 2012