

MARSH

Issues in Risk Management: Privacy and Data Breach

Understanding the Risk and Managing a Crisis



Leadership, Knowledge, Solutions...Worldwide.

Issues in Risk Management: Privacy and Data Breach



Robert Parisi
Senior Vice President, FINPRO
National Practice Leader for Tech/Telecom E&O and Network Risk
212.345.5924
robert.parisi@marsh.com

Agenda

- Breach Crisis Metrics and Management
- Risk Transfer
 - Risk Overview
 - Coverage Overview
 - Benchmarking
 - The Marsh Approach
 - The Underwriting Process





Will you become a statistic?

- Federal Trade Commission (FTC) Identity Theft Complaints
 - Some **11.1 Million Victims** were victimized by some sort of identity theft-related fraud circumstance in 2009. (Up from 9.9 Million in 2008)
 - Approximately 3.3% of the US Population
 - ID Theft Fraud is the **Number 1 complaint** by consumers for the 9th consecutive year.
 - 954,228 complaints in 2008 (Up from 840,183 in 2007)
- Many Victims do not know they are a victim or report their victimization
- Fastest growing white collar crime in America today.

AGE	Percentage
1-29	31%
30-39	23%
40-49	19%
50+	26%

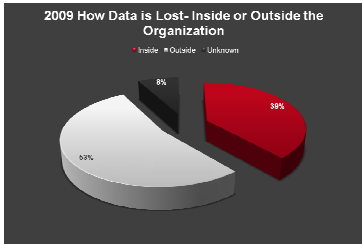
2009 How Data is Lost (General)

Inside Perpetrator (Accidental and Malicious Intent)

Category	Percentage
Accidental	75%
Malicious	25%

Source: <http://datalossdb.org/>

2009 How Data is Lost (General)
 Inside vs. Outside the Organization

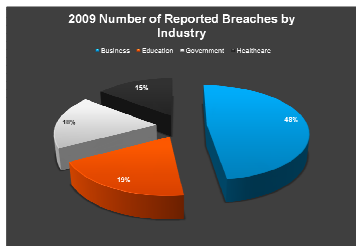


Source: <http://datalossdb.org/>



6

2009:
 Number of Reported Breaches by Industry

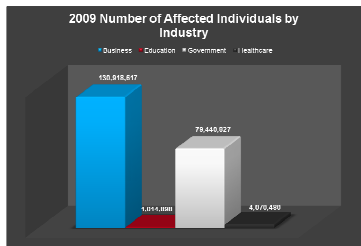


Source: <http://datalossdb.org/>



7

2009:
 Number of Reported Affected Individuals by Industry



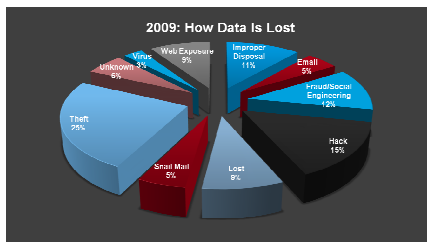
Source: <http://datalossdb.org/>



8

Data Breach Statistics

Data Loss by Type



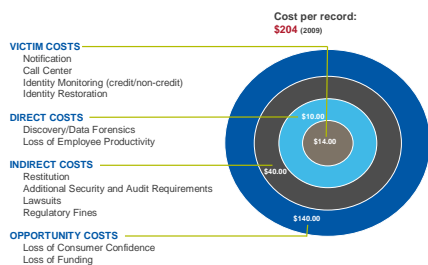
Source: <http://datalossdb.org/>



9

Breaches: By the numbers....

Cost of a breach record



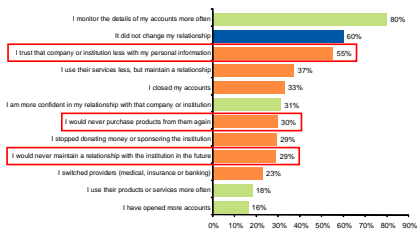
© Ponemon Institute



10

Breaches: By the numbers....

Consumer Confidence Survey



© Javelin Strategy & Research



11




What are the Risks?

- Privacy, computer and network security are not just Internet issues.
- Any entity that transacts business using:
 - a computer network; or
 - confidential information is at risk.
- 3000 B.C.
 - Chinese merchants disperse shipments so as to minimize the risk of total loss.

“Essentially, data loss is no longer a question of what if? The only question is when?”


Managing the Data Loss Crisis
By David Bartlett and Larry Smith
Risk Management Magazine, June 2008



13

What are the Risks?
Part II

- Legal liability to others for computer security breaches
- Legal liability to others for privacy breaches
- Regulatory actions and scrutiny
- Loss or damage to data / information
- Loss of revenue due to a computer attack
- Extra expense to recover / respond to a computer attack
- Loss or damage to reputation
- Cyber-extortion
- Cyber-terrorism



14

Threat Environment

- Social Media/Networking
- Internal:
 - Rogue employees
 - Careless staff
- External:
 - Organized crime:
 - Foreign
 - Domestic
 - Hackers
- Technology:
 - Hackers, viruses, etc
 - Structural vulnerability
- Old school:
 - Laptop theft
 - Dumpster diving
 - Phishing
- Regulatory



15

Risk Identification

Potential Risk Event	Likelihood	Potential Impact
Website copyright / trademark infringement claims	Low	Low
Legal liability to others for computer security breaches (non-privacy)	Low - Medium	Medium
Legal liability to others for privacy breaches	High	High
Privacy breach notification costs and credit monitoring	High	Medium
Privacy regulatory action defense and fines	Low	Medium
Costs to repair damage to your information assets	Low	Medium
Loss of revenue due to a failure of security or computer attack	Medium (overall) High (e-commerce)	Medium (overall) High (e-commerce)
Loss of revenue due to a failure of security at a dependent technology provider	Low	Medium
Cyber extortion threat	Low	Medium



16

Coverage Overview



What Are the Gaps in Traditional Policies?

- Traditional insurance was written for a world that no longer exists. Attempting to fit all of the risks a business faces today into traditional policy is like putting a round peg into a square hole.
 - Errors and Omissions (E&O): even a broadly worded E&O policy is still tied to “professional services” and often further tied to a requirement that there be an act of negligence
 - Commercial General Liability (CGL): covers only bodily and tangible property—Advertising Injury / Personal Injury (AI/PI) section has potential exclusions/limitations in the area of web advertising
 - Property: courts have consistently held that data isn’t “property”—“direct physical loss” requirement not satisfied
 - Crime: requires intent and only covers money, securities, and tangible property
 - Kidnap and Ransom (K&R): no coverage without amendment for “cyber-extortion”



18

Security & Privacy Insurance Policy Coverage Overview

Not covered Covered Not covered (dependent upon specifics of claims, may not be covered)

Privacy & Cyber Perils	Property	General Liability	Traditional Fidelity Bond	Computer Crime (not purchased only for P&I)	E&O (not purchased)	Special Risk	Broad Privacy & Cyber Policy
Destruction, corruption or theft of your electronic information (excludes data to backup of computer or network)							Information asset protection
Theft of your computer systems resources							Information asset protection
Business Interruption due to a material interruption in an element of your computer system due to breach of computer or network security (including data exposure and forensic support)							Network Business Interruption
Business Interruption due to your service provider suffering an outage as a result of a failure of the computer or network security							Network Business Interruption (admitted or approved based upon risk profile)
Identification of your notification costs, including credit monitoring services							Privacy Liability (sub-limited)
Defense of regulatory action due to a breach of privacy regulation							Privacy Liability (sub-limited)
Coverage for Fines and Penalties due to a breach of privacy regulation							Privacy Liability
Threats or extortion relating to release of confidential information or breach of computer security							Cyber Extortion
Liability resulting from disclosure of electronic information & electronic information assets							Network Operations Security
Liability from disclosure confidential commercial &/or personal information (a breach of physical)							Privacy Liability
Liability for electronic crimes suffered by others from a failure of your computer or network security (including written policies & procedures designed to prevent such occurrences)							Network Operations Security



19

Coverage Overview

- ✓ **Network security liability:** liability to a third party as a result of a failure of your network security to protect against destruction, deletion, or corruption of a third party’s electronic data, denial of service attacks against internet sites or computers; or transmission of viruses to third party computers and systems
- ✓ **Privacy liability:** liability to a third party as a result of the disclosure of confidential information collected or handled by you or under your care, custody or control. Includes coverage for your vicarious liability where a vendor loses information you had entrusted to them in the normal course of your business.
- ✓ **Crisis management and identity theft response fund:** expenses to comply with privacy regulations, such as communication to and credit monitoring services for affected customers. This also includes expenses incurred in retaining a crisis management firm for a forensic investigation or for the purpose of protecting/restoring your reputation as a result of the actual or alleged violation of privacy regulations.



20

Coverage Overview (continued)

- ✓ **Cyber extortion:** ransom or investigative expenses associated with a threat directed at you to release, divulge, disseminate, destroy, steal, or use the confidential information taken from the insured, introduce malicious code into your computer system; corrupt, damage, or destroy your computer system, or restrict or hinder access to your computer system.
- ✓ **Network business interruption:** reimbursement of your loss of income and / or extra expense resulting from an interruption or suspension of computer systems due to a failure of network security to prevent a security breach. Includes sub-limited coverage for dependent business interruption.
- ✓ **Data asset protection:** recovery of costs and expenses you incur to restore, recreate, or recollect your data and other intangible assets (i.e., software applications) that are corrupted or destroyed by a computer attack.



21

Privacy Liability

Why is it Different From Cyber Liability?

- **Breach of privacy:**
 - Disclosure of confidential information:
 - Personal
 - Commercial
 - Cause doesn't matter:
 - Negligence
 - Intentional acts
 - Computers
 - Vendors
 - Dumpsters
 - Phishing
 - Employees
- **Damages / covered loss:**
 - Legal liability
 - Defense and claims expenses
 - Regulatory defense costs
 - Vicarious liability when control of information is outsourced
- **Crisis coverage:**
 - Credit remediation, credit monitoring, and ID Theft investigation
 - Forensic expenses
 - Cover for crisis and public relations expenses
 - Cover for notification costs



22

Benchmarking



Other Litigation

- Minnesota. BCBS Plan Accidentally Prints a Member's Unredacted Claims Processing Form in Member Handbooks sent to 95,000 members.
 - SSN was not included.
 - Plan discovered error and notified member.
 - Discontinued use of the booklet, changed member's ID number, and offered credit monitoring.
 - Member filed lawsuit against plan in April 2010.
- Class action lawsuits pending in a number of jurisdictions based on privacy/security breaches.



27

Actual Paid Claims

- Wrongful disclosure of information by employee of credit union who sold information to outsiders.
 - Amount paid by insurer for liability claim and first party loss: **\$1.8 million**
- Third party computer hacker stole credit card information.
 - Amount paid by insurer for liability claim: **\$5 million** (note that this was the primary policy limit. Claim eroded excess limits as well)
- Third party computer hacker stole passwords by electronic means and used those passwords to gain access to personal information.
 - Amount paid by insurer for liability claim (class action): **\$8 million+**
- Employee sold customer data to others.
 - Amount paid by insurer for liability claim: **\$9.1 million**
- Employee stole and sold information to identity theft ring.
 - Amount paid by insurer for notice and liability claim: **\$2.6 million**
- Unauthorized access to database resulting from stolen passwords.
 - **\$4.5 million**
- Insured's employees released proprietary information of the claimant to third parties.
 - **\$715,000**

Source: Chartis



28

Actual Paid Claims (continued)

- Employee misappropriated confidential information from a competitor.
 - Amount paid by insurer for liability claim: **\$200,000**
- Rogue employee at medical provider stole and sold over 40,000 patient records containing Personally Identifiable Information.
 - Amount paid by insurer notification costs: **\$675,000**
- Insured lost tapes containing medical insurance information and SSNs.
 - Amount paid by insurer for call center services and credit monitoring costs: **\$400,000 + other pending costs**
- Rogue employee stole and sold customer data of over 3,000,000 customers to others.
 - Amount paid by insurer for liability claim and notification / credit monitoring: **\$7.1 million**
- Hotel network was hacked, gaining access to personally identifiable information.
 - Amount paid by insurer for notification costs, forensic investigation, crisis management, and credit monitoring: **\$420,000 + other pending costs**
- Insured accidentally published non-public student information on their website.
 - Amount paid by insurer for notification and credit monitoring costs: **\$100,000+**
- Employee of a college accidentally emailed personal information of over 20,000 students.
 - Amount paid by insurer for notification and call center costs: **\$38,000**

Source: Chartis




29



Risk Management


- Placement of coverage is the last step in the process
- Insurance is never a valid alternative to good risk management
- Similarly, relying upon technology as some mythical "silver bullet" that will defend against all risks is to turn a blind eye to major risks facing every commercial entity
- Marsh's approach to the privacy and cyber risks combines elements of:
 - **Assessment;**
 - Remediation;
 - Prevention;
 - Education; and
 - **Risk transfer.**



31

Assessment

- **Specialized privacy and information security assessment** to assist you in evaluating internal policies and procedures related to human, physical, and network security, privacy, and breach preparedness
- **Risk mapping:** once the privacy and information security assessment has been completed, Marsh works with you to identify your potential exposure to a breach—this includes a scorecard, a gap analysis of your breach response policies and procedures, and a risk map identifying and evaluating both the severity and probability of key privacy and information security risks
- **Benchmarking & Modeling:** going beyond simple matching you against what your peers do, Marsh will add a layer of benchmarking that details the costs and expenses associated with likely risk scenarios, including an analysis of a catastrophic privacy and information security event
- **Coverage gap analysis:** Marsh reviews your in force insurance policies to determine what coverage may be available to respond to claims and losses in the event of computer attack, breach of privacy, or loss of confidential information




32



Underwriting Process for E-Business Insurance

- Quote process:
- Application
- Security self-assessment:
 - Security ISO 27001/2
- Approach to underwriting is different by insurer
- Principal primary markets:
 - ACE – CNA
 - AXIS – CHUBB
 - Beazley – Hiscox
 - Chartis – KILN
- Market capacity: over \$400 million



34



Network, Cyber, Information Security, and Privacy Risk Group

- Recognized experts with deep technical skills:
 - Insurance industry thought leaders on cyber and privacy risk having drafted and / or consulted in the creation of all forms in the marketplace
 - Over two dozen professionals globally with experience in privacy and cyber risk
 - Combined team experience in addition to several decades of broking experience: two decades of law firm practice, nearly 50 years of underwriting
- Industry and product specialization:
 - Marsh's FINPRO team works with the industry practices to stay abreast of the unique concerns of specific industries
 - Marsh has led the market in placement of complex privacy and cyber coverage for Communications, Media, Technology, Internet, Financial Institution, Higher Education, Retail, and Health Care industry clients
- Strategic and transactional capabilities:
 - Access to domestic and foreign insurers as well as specialty excess markets
 - Coverage prioritization for all major insurers' policies
 - Deep bench strength in handling of accounts with brokers who have been placing these lines of coverage
 - Risk profiling and information assessment tools and services
 - Coverage gap analysis
 - Benchmarking tools that are adapted to size, industry, and nature of the risk / client
- Leading market relationships:
 - Marsh's practice leaders previously held management roles at most of the major insurers
 - Marsh places more cyber and privacy with more markets than any other broker



36



Data Breach Legal Issues

James H. Ferrick III
Jason L. Ross
Greensfelder, Hemker & Gale, P.C.

We Earn Our Reputation From The Companies We Keep®



Data Breach Regulation

- Historically
 - FERPA
 - The Financial Services Modernization Act of 1999 aka The Gramm-Leach-Bliley Act
- Recently
 - State Data Breach Statutes
 - FTC Red Flag Rules
 - HIPAA as amended by HITECH

We Earn Our Reputation From The Companies We Keep®



FERPA

- The **Federal Family Educational Rights and Privacy Act** of 1974, known as "FERPA," ([20 U.S.C. § 1232g](#); [34 C.F.R. Part 99](#)) governs access to student education records maintained by educational institutions.

We Earn Our Reputation From The Companies We Keep®



FERPA

- FERPA protects from disclosure "education records," broadly defined to include all records directly related to a student and maintained by an educational institution or someone acting on its behalf (e.g., contractors). Records can be in any format, including email messages, other computer records, videos, etc.
- However, the definition excludes, among other records:
 - campus law enforcement records (if certain criteria are met);
 - certain notes made by employees for their own personal use;
 - certain employment records;
 - certain medical treatment records; and
 - alumni records containing information obtained after a student's graduation.

We Earn Our Reputation From The Companies We Keep®



FERPA

- **Record of Disclosures**
 - As part of the education record of each student, each institution must maintain a record of disclosures which contains the following information:
 - The names of all individuals, agencies, or organizations that have requested, or obtained, access to the student's records and the legitimate educational interest of those accessing the information; and
 - Any disclosures that are made under the health and safety emergency exception, the circumstances surrounding that decision to disclose and to whom disclosures were made.

We Earn Our Reputation From The Companies We Keep®



FERPA Violations

- **FERPA Complaints.** Students may file a complaint with the U.S. Department of Education. Generally speaking, however, students may not file a lawsuit against the institution for a violation of FERPA.
- **Penalties for Violation of FERPA.** Penalties for uncorrected violations may include a cutoff of federal funding to the institution.

We Earn Our Reputation From The Companies We Keep®



The Gramm-Leach-Bliley Act

- THE GLBA requires financial institutions to carefully protect customers' financial information.
- Two components: 1) safeguard rules and (2) privacy rules.
- Under the Safeguards Rule, educational institutions, in their capacity as "financial institutions" must have in place a written information security program designed to:
 - ensure the security and confidentiality of customer records;
 - protect against any anticipated threats or hazards to the security of such records; and
 - protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to customers.

We Earn Our Reputation From The Companies We Keep®



The Gramm-Leach-Bliley Act

- FTC enforcement of the Safeguards Rule.
- The FTC has expressly stated that it considers educational institutions to be "financial institutions" subject to its jurisdiction for purposes of the GLBA because "[m]any, if not all, [educational] institutions appear to be significantly engaged in lending funds to consumers."
- Privacy Rule: Financial institutions must give their customers - and in some cases their consumers - a "clear and conspicuous" written notice describing their privacy policies and practices. When an entity provides notice and what it says depends on what is done with the information.
- Resource: <http://www.ftc.gov/privacy/glbact/index.html>

We Earn Our Reputation From The Companies We Keep®



State Data Breach Laws

- Forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information (as of October 12, 2010.)
- Complete Listing can be found @:
<http://www.ncsl.org/default.aspx?tabid=13489>
- See also Data Destruction Laws--
<http://www.ncsl.org/default.aspx?tabid=21075>

We Earn Our Reputation From The Companies We Keep®



State Data Breach Laws

- Every state law contains slight variances
- (1) what constitutes a security breach
 - (2) who must be notified following a breach;
 - (3) when must notification occur;
 - (4) what is considered protected information;
 - (5) what are the penalties for failure to notify.

We Earn Our Reputation From The Companies We Keep®



State Data Breach Laws

- What constitutes a security breach
- Acquisition (actual possession)
 - Access (e.g. hacker)
 - Access and Acquisition
 - Compromises vs. materially compromises security, confidentiality or integrity of data

We Earn Our Reputation From The Companies We Keep®



State Data Breach Laws

Who must be notified following a breach?

- Most states:
 - Affected individuals within state
 - If threshold met, consumer reporting agencies
- Other states:
 - One or more state agencies
 - All affected consumers regardless of residence if you do business in the state, see e.g. Wisconsin.
 - All affected consumers who live in the state regardless of the location of business, see e.g. Hawaii.

We Earn Our Reputation From The Companies We Keep®



State Data Breach Laws

When must notification occur?

- Most states: 45 days
- Puerto Rico: 10 days

We Earn Our Reputation From The Companies We Keep®



State Data Breach Laws

What is considered protected information?

- Most states:
 - unencrypted social security numbers
 - drivers license numbers
 - account numbers (along with passwords necessary to access those accounts)
- Other states are more broad:
 - “biometric data” e.g. DNA
 - Hawaii—any record regardless of physical form or characteristic

We Earn Our Reputation From The Companies We Keep®



State Data Breach Laws

What are the penalties for failure to notify?

– Most states:

- Fine ranging from daily penalties up to \$150,000.
- Attorney General has exclusive jurisdiction.

– Other states are more broad:

- Private right of action—e.g. California, Hawaii, Louisiana, New Hampshire, North Carolina, Tennessee and Washington

– Per breach vs. Per Affected Consumer

We Earn Our Reputation From The Companies We Keep®



FTC RED FLAGS RULE

Red Flags Rule requires many businesses and organizations to implement a written Identity Theft Prevention Program designed to detect the warning signs – or “red flags” – of identity theft in their day-to-day operations, take steps to prevent the crime, and mitigate the damage it inflicts.

We Earn Our Reputation From The Companies We Keep®



FTC RED FLAGS RULE

- Red Flags Rule—effective January 1, 2008
- Implements sections 114 and 315 of the Fair and Accurate Credit Transaction Act (FACT) of 2003.
- Enforcement began January 1, 2011
- Red flags are suspicious patterns or practices, or specific activities, that indicate the possibility of identity theft.
- Red Flags Rule was modified by legislation in late 2010— not likely to affect colleges and universities.

We Earn Our Reputation From The Companies We Keep®



FTC RED FLAGS RULE

- Colleges and Universities are covered.
 - an entity is a creditor if it regularly and in the ordinary course of business does one or more of the following:
 - 1) obtains or uses consumer reports, directly or indirectly, in connection with a credit transaction;
 - 2) furnishes information to consumer reporting agencies in connection with a credit transaction; or
 - 3) advances funds to or on behalf of a person, based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person.
 - University loan programs, admissions, job applications etc.

We Earn Our Reputation From The Companies We Keep®



Red Flag Program Requirements

- Program must include reasonable policies and procedures to identify the "red flags" of identity theft entity may run across in the day-to-day operation of its business.
- Program must be designed to detect the red flags entity has identified.
- Program must spell out appropriate actions to be taken when red flags are detected.
- Program must address updates and reevaluation due to ever-changing threat.

We Earn Our Reputation From The Companies We Keep®



Red Flag Rule Additional Requirements

- Board of Directors must approve initial version.
- Program must identify person responsible for implementing and administering.
- Program must set forth staff training.
- Program must address vendor compliance.

We Earn Our Reputation From The Companies We Keep®



FTC RED FLAGS RULE

- Rule allows for flexibility in the scope of the Identity Theft Prevention Program. Factors to consider include:
 - creditors' activities; and
 - level of identity theft risk associated with the relevant covered accounts.
- Determination of risk will be largely based on past experience.
- Entities can tailor program appropriately
- Identity Theft Program:
 - Written
 - Duly Approved
 - Implemented
 - Updated
 - Not Detailed or Complex
- FTC RESOURCE:
<http://www.ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml>

We Earn Our Reputation From The Companies We Keep®



HIPAA & HITECH

- Health Insurance Portability and Accountability Act (HIPAA) imposes obligations on health plans, health care clearinghouses, and health care providers to protect health information when electronically transmitted. (1996)
- The Health Information Technology for Economic and Clinical Health Act (HITECH) addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of HIPAA. (2009)

We Earn Our Reputation From The Companies We Keep®



HIPAA Privacy Rule

- The Privacy Rule assures that health information is properly protected while allowing the flow of health information needed to provide and promote health care.
- The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral, commonly called "protected health information" or PHI.
- The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek medical care.
- Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed.
- The Privacy Rule permits certain incidental uses and disclosures that occur as a by-product of another permissible or required use or disclosure, as long as the covered entity has applied reasonable safeguards and implemented the minimum necessary standard, where applicable, with respect to the primary use or disclosure. See 45 CFR 164.502(a)(1)(iii).
- Link: <http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html>

We Earn Our Reputation From The Companies We Keep®



HIPAA Security Rule

- The Security Rule establishes a national set of security standards for protecting certain health information that is held or transferred in electronic form.
- **ENCRYPTION CAN BE A SAFE HARBOR IN EVENT OF BREACH**
 - As long as PHI is not encrypted, it is considered unsecured.
 - *HITECH's* breach notification requires covered entities to send notification letters if there is a breach of unsecured PHI. Encryption grants safe harbor in the event of a breach because encrypted PHI is not unsecured PHI.
 - Different Standards: DATA IN MOTION vs. DATA AT REST
 - HHS defers to the following National Institute of Standards and Technology (NIST) requirements which normally apply only to government entities.
 - Safe harbor if, and only if, entity adheres to strict standards and guidelines. Encrypted data is meaningless without taking into account the NIST requirements. By proactively leveraging the proper encryption technologies, companies of all sizes can avoid these breach notifications while ensuring the security of their sensitive data
- **There is no silver bullet.** In the event of a breach, Entity is required to notify HHS, the patient, and in some cases, the media.
- Vendors are covered—Business Associate Agreements must be in place

We Earn Our Reputation From The Companies We Keep®



HITECH BREACH NOTIFICATION

- HIPAA did not require notice of violations.
- HITECH requires notice to:
 - Individual or next of Kin
 - substitute notice (when insufficient information to make direct notice) in the case of 10 or more individuals by posting on the home page of the entities' Web site or notice in major print or broadcast media.
 - when possibility of imminent misuse of the unsecured PHI, notice by telephone or other method is permitted in addition.
 - Notice to prominent media outlets within the State or jurisdiction if a breach of unsecured PHI affects or is reasonably believed to affect more than 500 residents of that State or jurisdiction.
 - Notice to the Secretary of HHS immediately for breaches involving more than 500 individuals and annually for all other breaches.
 - Posting an HHS Web site of a list that identifies each entity involved in a breach in which the unsecured PHI of more than 500 individuals is acquired or disclosed.
- Notification in 60 days.
- Vendors must notify the Covered Entity.

We Earn Our Reputation From The Companies We Keep®



HIPAA PENALTIES

- No private right of action.
- Complaints must be filed within 180 days of violation.
- Fine of up to \$50,000
- Criminal Liability--\$250,000 fine/10 years
- State attorneys general now empowered to bring an enforcement action for HIPAA violations

We Earn Our Reputation From The Companies We Keep®



Best Practices--Breach

- Treat every instance in which an unauthorized individual views, or has the opportunity to view, personal information as a data-security breach for internal purposes.
- Immediately initiate an investigation to evaluate the threat of harm from any data-security breach.
- Notify your state's law enforcement officials if there is any reason to believe that the incident may result in identity theft or other misuse of the information.
- If maintaining information on behalf of another, immediately notify the owner or licensee of that information of the security breach.
- If there is a reason to believe that the incident may result in the misuse of information, notify necessary governmental agencies within 45 days (10 days in certain circumstances) of the breach that you intend to disclose the breach to consumers.
- If there is a reason to believe that the incident may result in the misuse of information, notify consumers in less than 45 days.
- If there is no reason to believe that the incident may result in the misuse of information, prepare a written document describing the scope and findings of the investigation and maintain that document for at least five years. Review the laws of all of the states in which affected consumers reside to determine if a limited notification may still be required to either consumers or government agencies under certain state laws, or if documentation concerning your determination must be provided to state agencies.
- If you send notice to more than 500 consumers, notify the consumer reporting agencies.
- Notify all involved to preserve all data, correspondence, emails etc to prevent loss of evidence in order to aid in defense and avoid charge of spoliation of evidence.

We Earn Our Reputation From The Companies We Keep®



Best Practices Data Breach Prevention

- **Conduct a Risk Assessment**
Know the network's vulnerabilities, i.e. what type of information might get exposed, who might expose it, how and where it could be exposed, and what applications use it.
- **Categorize the Data**
Establish a classification standard: Confidential, restricted and public. Sensitive, private or other mid-levels can be added if needed.
- **Determine Who Has Access**
Determine who has access to various types of data, and access should be granted on a need-to-know basis.
- **Manage Your Personnel**
Common misperception: assuming employees do not constitute a threat.
- **Control the Administrator Rights**
Control the administrator rights of a computer reduces the chances of an insider intentionally or unintentionally downloading malware or malicious code.
- **Take a Multi-Layer Approach**
Must account for PCs, laptops, cell phones, thumb drives, PDAs etc. and the network—it is about the information not the device. Also layer protection by having firewalls, anti-virus software, anti-spam, intrusion prevention (IPS), network access control (NAC) etc those activities.

We Earn Our Reputation From The Companies We Keep®



Best Practices Data Breach Prevention

- **Encrypt Information**
Encrypt information at the point of entry, i.e. at the application layer so that the data defends itself as it travels. Encrypt laptop hard disks and other portable devices is also recommended.
- **Maintain Physical Access Control**
Control physical access, including simple solutions like locking office doors, installing card access control, locking a device to a work station, locking filing cabinets, logging off a computer or having an auto log off functionality. Consider anti-theft solutions that remotely track the location of a stolen laptop or swipe a device clean.
- **Dispose of Records Properly**
Shred, burn or pulverize paper files. Additionally, disks, DVDs and old computers should be erased before being discarded. Specific state statutes on data destruction.
- **Implement Policies**
Implement and educate employees on the security policies of a campus, why they are important and how to protect confidential information—address telecommuting and home computers
- **Manage Your Vendors**
Ensure Vendor compliance.

We Earn Our Reputation From The Companies We Keep®



Issues in Risk Management Privacy and Cyber Liability

The information contained herein is based on sources we believe reliable, but we do not guarantee its accuracy. Marsh makes no representations or warranties, expressed or implied, concerning the application of policy wordings or of the financial condition or solvency of insurers or reinsurers. The information contained in this publication provides only a general overview of subjects covered, is not intended to be taken as advice regarding any individual situation, and should not be relied upon as such. Statements concerning tax and/or legal matters should be understood to be general observations based solely on our experience as insurance brokers and risk consultants and should not be relied upon as tax and/or legal advice, which we are not authorized to provide. Insureds should consult their own qualified insurance, tax and/or legal advisors regarding specific coverage and other issues.

All insurance coverage is subject to the terms, conditions and exclusions of the applicable individual policies. Marsh cannot provide any assurance that insurance can be obtained for any particular client or for any particular risk.

This document or any portion of the information it contains may not be copied or reproduced in any form without the permission of Marsh Inc., except that clients of any of the companies of MMC need not obtain such permission when using this report for their internal purposes, as long as this page is included with all such copies or reproductions.

Marsh is part of the family of Marsh & McLennan Companies, including Guy Carpenter, Mercer, and the Oliver Wyman Group (including Lippincott and NERA Economic Consulting).

Copyright 2011 Marsh Inc.
All rights reserved.



66

MARSH



Leadership, Knowledge, Solutions...Worldwide.