



Minnesota Society for Healthcare Risk Management September 22, 2011

Cyber and Privacy Risk – What Are the Trends? Is Insurance the Answer?

**Melissa Krasnow, Partner, Dorsey & Whitney, and
Certified Information Privacy Professional**

Sharon Scharf, Senior Vice President, Marsh FINPRO

This presentation was created by Dorsey & Whitney LLP, 50 South Sixth Street, Suite 1500, Minneapolis, MN 55402. This presentation is intended for general information purposes only and should not be construed as legal advice or legal opinions on any specific facts or circumstances. An attorney-client relationship is not created or continued by sending and/or receiving this presentation. Members of Dorsey & Whitney will be pleased to provide further information regarding the matters discussed in this presentation.

Breaches

- **Breaches and incidents frequently occur, are reported and publicized by the media and on the internet**
- **Legal issues and business considerations**
- **Data crosses country borders**

State breach notification laws

- **Cover personal information, meaning name, plus any of:**
 - **social security number**
 - **driver's license number**
 - **financial account information (e.g., credit card, bank account, etc.)**
 - **in some cases, health information**

State breach notification laws

- **Notification an entity must make for breach of personal information to affected state residents and, in some cases:**
 - **state attorney generals**
 - **state regulators**
 - **credit reporting agencies**
- **Timing of notification varies according to state breach notification law**
- **Amendments to state breach notification laws**

Enforcement of state breach notification laws varies

- **State attorney general enforcement in Minnesota**
- **Private right of action in California**
- **Administrative fines in Florida**

Massachusetts privacy regulation

- **Covers any entity (regardless of whether in Massachusetts or whether already complies with the federal HIPPA / HITECH Act) with access to Massachusetts resident personal information**
- **Written information security program (WISP) is required**
- **Reporting a breach to the Massachusetts attorney general (which is required under the Massachusetts breach notification law) could trigger an investigation of a reporting entity, including that the entity submit its WISP for review**
- **2011 Massachusetts attorney general privacy enforcement actions**

Massachusetts privacy regulation

- **Requires written information security program mandating encryption of personal information transmitted wirelessly and stored on portable devices**
- **Revisit applicable company policies (e.g., technology and electronic communications):**
 - **Company access to and monitoring of employee-owned devices**
 - **Applicability to company and employee-owned mobile devices**

State social security number laws

- **Could be implicated in a breach involving social security numbers**

Federal HIPAA / HITECH Act breach notification

- **Applies to covered entities and business associates**
- **Covered entity means (i) health plan, (ii) health care clearinghouse or (iii) health care provider**
- **Business associate that (i) on behalf of a covered entity, performs activity involving use or disclosure of individually identifiable health information or (ii) provides legal, actuarial, accounting, consulting, management, administrative, accreditation or financial services for the covered entity involving the disclosure of individually identifiable health information from the covered entity to the person**

Federal HIPAA / HITECH Act breach notification

- **Protected health information means individually identifiable health information relating to health care treatment, a health condition or payment for the provision of health care**
- **Covered entity notification to each individual, U.S. Department of Health and Human Services (if breach involves more than 500 individuals) and prominent media outlet (if breach involves more than 500 residents of state or jurisdiction)**
- **Business associate notification to covered entity**

Enforcement of federal HIPAA / HITECH Act

- **U.S. Department of Health and Human Services enforcement**
- **Civil penalties**
- **Criminal penalties**
- **State attorney generals also can bring civil actions**
- **No private right of action**

Review information and documentation and determine applicable laws

- **Personally identifiable information – what, where and in which form is it?**
- **Which company policies and procedures and agreements have provisions relating to privacy and confidentiality?**
- **Determine which laws apply and what the requirements are (e.g., policies and procedures and agreements)**
- **Sometimes, policies and procedures are advisable, though not required by law**
- **Which federal and state and other laws apply?**

Be prepared

- **Prepare policies and procedures and ensure they are consistent and integrated with company policies and procedures**
- **Devise a roadmap of what to do in the event of a possible breach**
- **Consider handling of investigations**
- **How should a company respond internally and externally to media, employees and others about breach circumstances and status?**
- **Is SEC disclosure required for a public company?**

A solid, light brown square with rounded corners, positioned to the left of the main title box.

Network Security and Privacy Insurance

Sharon Scharf
sharon.k.scharf@marsh.com

What are the risks?

Privacy, computer, and network security are not just Internet issues.

- Any entity that transacts business using:
 - a computer network
 - confidential information is at risk

The question is no longer “if” you will experience a privacy or data breach, but “when.”

The risks all companies face:

- 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

Threat Environment

- **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**

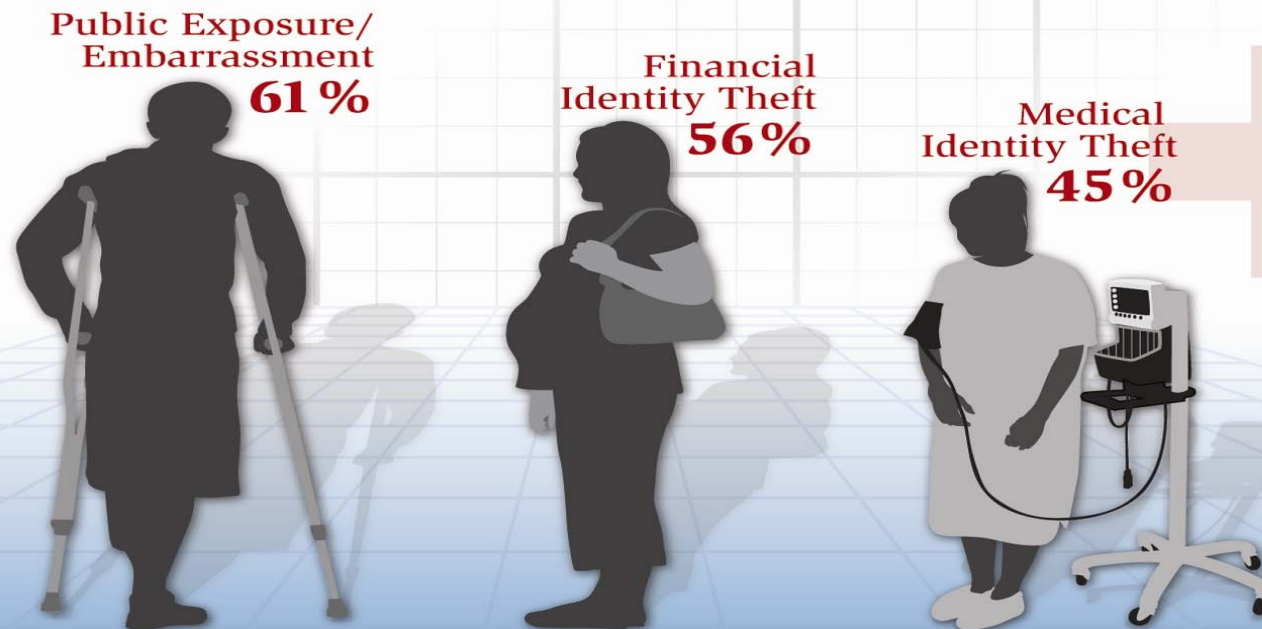
Trends

- Electronic health records
- The number of healthcare breaches in 2010 have outpaced other verticals -- including banking and government -- by as much as threefold
- Sixty percent of organizations in recent study had more than two data breaches in the past two years. The average number for each participating organization was 2.4 data breach incidents.
- The economic impact of a data breach over the past two years is approximately \$2 million.
- Forty-one percent of respondents were made aware of data breach as a result of a patient complaint.

Ponemon Institute: 2010 Benchmark Study on Patient Privacy and Data Security

Top Risks

Top Risks Patients Face When Their Data Is Breached



Source: Ponemon Institute and ID Experts, Benchmark Study on Patient Privacy and Data Security, November 2010. Question: In your opinion, what harms do patients actually suffer if their records are lost or stolen?

What are the Exposures and Risks?

- Investigate the breach
- Crisis management
- Determine statutory obligations
- Provide written notification
- Offer complimentary credit monitoring
- Provide identity theft relief services
- Regulatory actions and scrutiny (Defense costs & penalties)
- Costs re-create and determine what data was contained in databases
- Legal liability to others for privacy breaches (Defense costs & damages)

Cost? - Marsh Data Breach Modeling

Privacy Event Modeling

Potential Value of a Privacy Event

Based upon number of records compromised

Number of Records Compromised	50,000	250,000	500,000	1,000,000
Privacy Notification Costs	\$150,000	\$750,000	\$1,500,000	\$3,000,000
Call Center Costs	\$50,000	\$250,000	\$500,000	\$1,000,000
Credit Monitoring Cost	\$300,000	\$1,500,000	\$3,000,000	\$6,000,000
ID Theft Repair	<u>\$250,000</u>	<u>\$1,250,000</u>	<u>\$2,500,000</u>	<u>\$5,000,000</u>
Total Estimated 1st Party Costs*	\$750,000	\$3,750,000	\$7,500,000	\$15,000,000
Card Reissuance Liability	\$300,000	\$1,500,000	\$3,000,000	\$6,000,000
Fraud Liability	<u>\$2,500,000</u>	<u>\$12,500,000</u>	<u>\$25,000,000</u>	<u>\$50,000,000</u>
Total Estimated 3rd Party Liability	<u>\$2,800,000</u>	<u>\$14,000,000</u>	<u>\$28,000,000</u>	<u>\$56,000,000</u>
TOTAL ESTIMATED PRIVACY EVENT	\$3,550,000	\$17,750,000	\$35,500,000	\$71,000,000

* May be subject to a Privacy Event Cost Sublimit

Assumptions:

Notification costs - \$3 per record

Call Center Costs - \$5 per call (20% expected participation)

Credit monitoring - \$30 per record (20% expected participation)

ID Theft Repair - \$500 per record (5% of those monitored experience theft)

Card re-issuance - \$6 per record (potential liability to issuers i.e. banks)

Fraud Liability - \$1,000 per record (range is \$500 per record to \$6,400 average fraud charges - 5% experience fraud)

Breach Example

July 17, 2010

Hospital: 800,000 records containing sensitive, personal health, and financial information were compromised when Hospital's data management company lost backup tapes containing copies of the hospital's most sensitive databases created between 2006 and early 2010. The files were slated for destruction prior to loss. They contained the mother lode for potential identity thieves: names, addresses, phone numbers, dates of birth, Social Security numbers, patient health information, and even bank account data.

Attorney General and OCR Enforcement

- January 13, 2010
State Attorney General filed suit against Managed Care Organization, which lost a portable external hard drive containing 7 years of data for 446,000 state residents.
 - Demanded identity theft insurance, reimbursement for credit freezes, and credit monitoring for 2 years
 - Sought \$5,000 per violation, court costs and attorney fees
 - On July 6, 2010, entity agreed to pay \$250,000 to resolve alleged violations. Amount would increase to \$500,000 if later determined that data was misused and 250 or more individuals file claims of identity theft.
 - “Corrective Action Plan” in which entity is implementing several detailed measures to protect health information and other private data in compliance with HIPAA. This plan includes continued identity theft protection, improved systems controls, improved management and oversight structures, improved training and awareness for its employees, and improved incentives, monitoring, and reports.

Attorney General and OCR Enforcement

- July 2010
National Pharmacy agrees to pay OCR \$1 million to settle complaint involving improper disposal of prescriptions and pill bottles.
 - Also agreed to a 3 year corrective action plan
 - Signed a consent order with the FTC which will be in place for 20 years. Order requires external, independent assessments of its stores' compliance.

Fines & Penalties

California Department of Public Health (“CDPH”): AB 211 & SB 541

- Community Hospital: The hospital was assessed a \$250,000 fine after the facility failed to prevent unauthorized access of 204 patients’ medical information by one employee.
- Memorial Hospital: The hospital was assessed a \$100,000 fine after the facility failed to prevent unauthorized access of 33 patients’ medical information by 17 employees.
- Medical Center: The hospital was assessed a \$130,000 fine after the facility failed to prevent unauthorized access of one patient’s medical information by seven employees.

Other Litigation

- Health Insurer Accidentally Prints a Member's Un-redacted 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.

Actual Paid Claims

- Employee sold customer data to others.
 - Amount paid by insurer for liability claim: \$9.1M.
- Employee stole and sold information to identity theft ring.
 - Amount paid by insurer for notice and liability claim: \$2.6M
- 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: \$7.1M.

Source: Chartis

A graphic consisting of a solid olive-green square on the left and a dark red rounded rectangle on the right. The text "Risk Transfer" is written in white, bold, sans-serif font inside the red rectangle.

Risk Transfer

Risks and Coverage

Risks	Coverage	Traditional Policies	Cyber & Privacy Policy
Legal liability to others for privacy breaches	Privacy Liability: Harm suffered by others due to the disclosure of confidential information		
Legal liability to others for computer security breaches	Network Security Liability: Harm suffered by others from a failure of your network security		
Extra expense to recover/respond to a computer attack	Cyber Extortion: The cost of investigation and the extortion demand		
Loss or damage to reputation			
Identity Theft	Expenses resulting from identity theft		
Privacy Notification Requirements	Cost to comply with privacy breach notification statutes		
Regulatory Actions	Legal defense for regulatory actions		

KEY: No coverage available Coverage may be available (“grey area”) Coverage Available

Network Security and Privacy Insurance Overview


- Network Security Liability
- Privacy Liability
- Crisis Management and Identity Theft Response Fund
- Cyber Extortion
- Network Business Interruption
- Data Asset Protection


What is Network Security/Privacy Insurance?



- Network Security Liability:** Liability to a third party as a result of a failure of network security to prevent or mitigate a computer attack, whether that attack originated internally or externally.
- Privacy Liability:** Liability to a third party as a result of an unauthorized disclosure of confidential information in your care, custody or control and/or a violation of privacy regulations—includes vicarious liability for actions of vendors to whom you have entrusted confidential information.
Note: Coverage for Network Security and Privacy Liability requires no negligence on the part of the insured and provides coverage for the intentional acts of insured's employees.
- Crisis Management and Identity Theft Response Fund:** Expenses to comply with privacy regulations, such as communication to and privacy response services for affected individuals—this also includes expenses incurred in retaining a crisis management firm for the purpose of protecting/restoring reputation as a result of the actual or alleged violation of privacy regulations as well as forensic investigation expenses.
- Cyber Extortion:** Ransom and investigative expenses associated with a threatened computer attack or privacy breach.

= Recommended coverage = Generally considered optional coverage

What is Network Security/Privacy Insurance?

 **Network Business Interruption:** Reimbursement of loss of income and/or extra expense resulting from an interruption or suspension of your computer system due to a failure of network security or system failure.

 **Data Asset Protection:** Costs to recollect, restore, or recreate electronic data, software or other applications that have been altered, corrupted, destroyed, deleted, or damaged by a computer attack.

 = Recommended coverage  = Generally considered optional coverage

Coverage Overview With Examples and Insurance Market Capacity

Coverage	Example	Limit of Liability	Retention
Network Security Liability	Hacking, virus transfer	Up to \$350,000,000	\$25,000 and up
Privacy Liability	Customer information breach	Up to \$350,000,000	\$25,000 and up
Privacy Breach Notification Costs	State privacy laws require notification	Up to \$70,000,000 or 10,000,000 records	Ranges from NIL and up
Crisis Management and Identity Theft Response Coverage	Credit monitoring and forensics	Up to \$10,000,000	Ranges from NIL and up
Data Asset Protection	Rebuild your damaged data from computer attack	Up to \$100,000,000	\$25,000 and up
Network Business Interruption	Loss of revenue due to computer attack	Up to \$100,000,000	A combination of the greater of \$25,000 + or 8 to 12 hours
Cyber Extortion	Ransom	Up to \$350,000,000	Ranges from NIL and up
Defense Costs/Fines and Penalties for Regulatory Actions	FTC or AG claims for privacy breach	Up to \$35,000,000	Ranges from NIL and up

Resources on Data Security Breach

- **FTC** – www.ftc.gov/bcp/edu/microsites/infosecurity/slides.pdf
- **Privacy Rights Clearinghouse** – www.PrivacyRights.Org
- **Open Security Foundation** – www.opensecurityfoundation.org
or www.datalossdb.org
- **Ponemon Institute, LLC.** – www.ponemon.org

Any Questions?

Dorsey & Whitney

Melissa Krasnow

Partner, Dorsey & Whitney,
and Certified Information

Privacy Professional

(612) 492-6106

krasnow.melissa@dorsey.com

Marsh

Sharon Scharf

Senior Vice President,

Marsh FINPRO

(612) 692-7888

sharon.k.scharf@marsh.com

Legal Disclaimer

This information is not intended to be taken as advice regarding any individual situation and should not be relied upon as such. Statements concerning tax, accounting and/or legal matters are general observations based solely on our experience as insurance brokers and risk consultants and should not be relied on as legal, tax or accounting advice. You should contact your legal, accounting, tax and other advisors regarding specific coverage and other issues. The information contained in this publication is based on sources we believe reliable but we make no representation or warranty as to its accuracy. 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. Marsh makes no representations or warranties, expressed or implied, concerning the application of policy wordings or the financial condition or solvency of insurers or re-insurers.

The hypothetical case studies contained herein are for illustrative purposes only and should not be relied upon as governing any specific facts or circumstances. All policy terms, conditions, limits, and exclusions are subject to individual underwriting review and are subject to change. Marsh cannot provide any assurance that insurance can be obtained for any particular client or for any particular risk. The hypothetical claims scenarios contained herein are for illustrative purposes only and should not be relied upon as governing any specific facts or circumstances. Actual claims are governed by the specific policy terms, conditions, limits, and exclusions and are subject to individual claims review by applicable insurer representatives.

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 Marsh & McLennan Companies need not obtain such permission when using this report for their internal purposes so 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.