

Who Needs Cyber Insurance?

A Review of Insurable Privacy Exposures Today

George N. Allport
Chubb Specialty Insurance
And

Steven H. Anderson
XL Insurance



Antitrust Notice



- The Casualty Actuarial Society is committed to adhering strictly to the letter and spirit of the antitrust laws. Seminars conducted under the auspices of the CAS are designed solely to provide a forum for the expression of various points of view on topics described in the programs or agendas for such meetings.
- Under no circumstances shall CAS seminars be used as a means for competing companies or firms to reach any understanding – expressed or implied – that restricts competition or in any way impairs the ability of members to exercise independent business judgment regarding matters affecting competition.
- It is the responsibility of all seminar participants to be aware of antitrust regulations, to prevent any written or verbal discussions that appear to violate these laws, and to adhere in every respect to the CAS antitrust compliance policy.

Chubb & Son, a division of Federal Insurance Company

Slide 2

Legal Disclaimer

The views, information and content expressed herein are those of the authors and do not necessarily represent the views of any insurers of the Chubb Group of Insurance Companies or of XL Insurance.

This presentation is advisory in nature and necessarily general in content. No liability is assumed by reason of the information provided.

Whether or not or to what extent a particular loss is covered depends on the facts and circumstances of the loss and the terms and conditions of the policy as issued.

The precise coverage afforded is subject to the terms and conditions of the policies as issued.

The information provided should not be relied on as legal advice or a definitive statement of the law in any jurisdiction. For such advice, an applicant, insured, listener or reader should consult their own legal counsel.

Chubb & Son, a division of Federal Insurance Company

Slide 3

Caring Hands Hospital System
 A Unit of CH Healthcare, Inc.

Search

Physician Finder Conditions & Treatments Hospital Guide Quality Report Card About Us

→ Contact Us **Health Library**
 → Get Directions Health Learning Centers
 → Request an Appointment Drug Information
 → Pay Your Bills Virtual Library
 → Contribute Podcasts
 → Find a Job Health Encyclopedia
 Health References

Caring Hands Celebrates "Teach Your Child to Cook Month" **Tour The New ED**

News
 Spring Air Borne Allergy Symptoms for Millions
 The change of season signals the start of spring allergies for an estimated 43 million Americans.

© 2010 Press Release


Chubb & Son, a division of Federal Insurance Company Slide 4

"The Cyber ID Thief"

On a "black hat" website, Myra learns how to write a SQL Injection script that allows her to gain access to Caring Hands databases through their website.

She is able to access and download over the Internet names, addresses and Social Security numbers of 11,500 CH patients. She then sells the information to mobsters in Eastern Europe.

Caring Hands, in accordance with HIPAA, notifies their patients of the "breach".



Chubb & Son, a division of Federal Insurance Company Slide 5

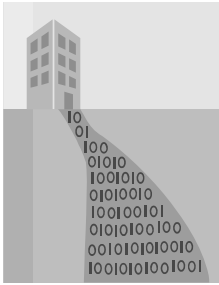
Data Breaches – Growing In Number!

Between January 10th, 2005 and March 6th, 2011

515,002,269

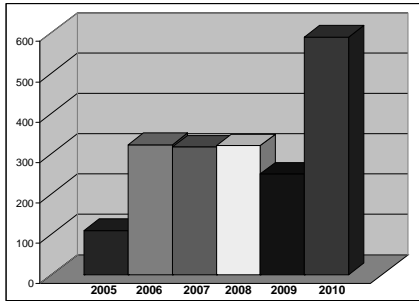
records containing "sensitive personal information" have been involved in security breaches!

Source: Privacy Rights Clearinghouse
 A Chronology of Data Breaches
 Updated March 8th, 2011
www.privacyrights.org



Chubb & Son, a division of Federal Insurance Company Slide 6

Number of Data Breaches

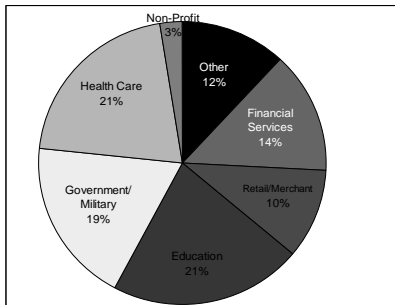


Privacy Rights Clearinghouse, Chronology of Data Breaches

Chubb & Son, a division of Federal Insurance Company

Slide 7

Data Breaches By Industry (2007 – 2010)

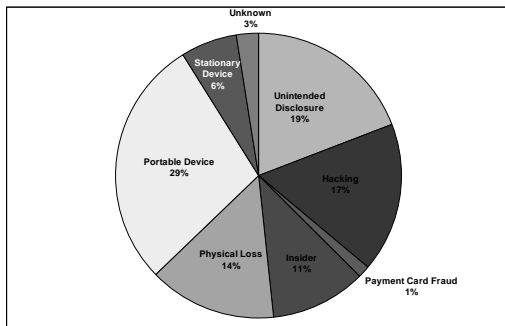


Privacy Rights Clearinghouse, Chronology of Data Breaches

Chubb & Son, a division of Federal Insurance Company

Slide 8

Breaches By Cause (2007-2010)



Privacy Rights Clearinghouse, Chronology of Data Breaches

Chubb & Son, a division of Federal Insurance Company

Slide 9

So, Why Does Caring Hands Care?

A Look At Some Privacy Laws!



Chubb & Son, a division of Federal Insurance Company

Slide 10

State Statutes

California first state to enact "security breach notification" legislation – July 1, 2003 [SB 1386].

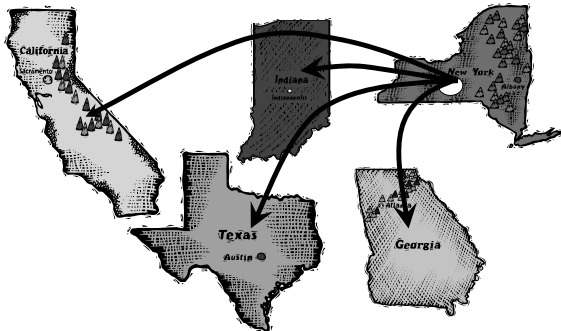
Currently, 46 other states have enacted *some type* of security breach notification legislation, including:

- Connecticut, Delaware, Florida, Georgia, Idaho, Illinois, Indiana, Maine, Massachusetts, Minnesota, Montana, New Hampshire, New Jersey, New York, Ohio, Oregon, Pennsylvania, Rhode Island, Texas, Vermont, Washington and Wyoming.

Chubb & Son, a division of Federal Insurance Company

Slide 11

The Reach Of The Laws



Chubb & Son, a division of Federal Insurance Company

Slide 12

“Personal Information” Examples

Illinois and District of Columbia don't require that a security code be accessed along with a credit or debit card number.

Oregon includes Passport number or other United States issued identification number.

California, along with **Missouri**, includes “medical information” and “health insurance information”.

Kansas and Maryland don't define “personal information”.

Methods of Notification

- Written (I.e. first class mail);
- Electronic (I.e. email);
- Telephonic;
- Substitute;
 - Email;
 - Notice on Website; and
 - Notice to, or in, Media.

HIPAA Update - 2009

- Requires notification within 60 days of a privacy breach involving an individual's HIPAA-covered personal health information
- Requires business associates to meet most security requirements that previously applied only to covered entities.
- Authorizes state attorneys general to bring suit for HIPAA violations
- Requires notification of the Department of Health & Human Services and the media in privacy breaches involving 500 or more individuals.

Gramm-Leach-Bliley Act

Financial Services Modernization Act of 1999 requires that financial institutions:

- "ensure the security and confidentiality of customer records and information;
- protect against anticipated threats or hazards to the security or integrity of such records;
- and protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."

Generally criticized by privacy advocates because enforcement rests solely with Federal regulators and the individual has no private right of action.

Typical Breach Related Expenses



Forensics

- Legal Expenses for Outside Attorney
- Cost of Forensic Examination
- Cost To Remediate Discovered Vulnerabilities



Notification

- Legal review and assessment
- Crafting letter or other notification
- Printing or design
- Mailing or other transmission
- Call Center Operations



Public Relations

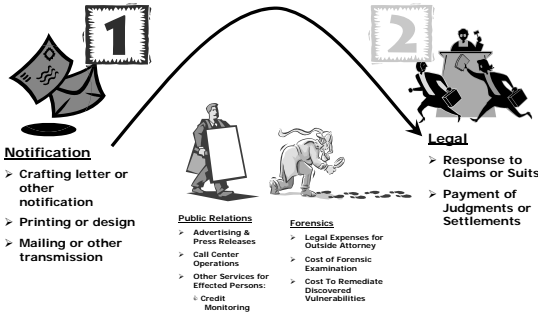
- Advertising & Press Releases
- Services for Affected Persons:
 - ↳ Credit Monitoring

Breach Costs By Activity

2009 Annual Study: Cost of a Data Breach: Ponemon Institute, LLC, January, 2010

<u>Activity</u>	<u>Percent</u>	<u>Dollar</u>
Outbound Contact	6%	\$12
Public Relations/Communications	1%	\$2
Inbound Contact	5%	\$10
Legal Services - Defense	14%	\$29
Identity Protection Services	2%	\$4
Investigation & Forensics	8%	\$16
Audit & Consulting Services	12%	\$24
Legal Services - Compliance	2%	\$4
Free or Discounted Services	1%	\$2
Lost Customer Business	40%	\$82
Customer Acquisition Cost	9%	\$18
Total	100%	\$203

"Notification" – Then "Litigation"



Damages – An Obstacle For *Persons*

- Loss of wages due to time taken to prove "identity theft" to MasterCard and Visa;
- Expense of legal and other resources necessary to prove "identity theft" to MasterCard and Visa;
- Loss of business advantage due to effect of fraudulent charges on FICO scores;
- Fear, emotional distress, mental anguish



Whose Fault Is It, Anyway?

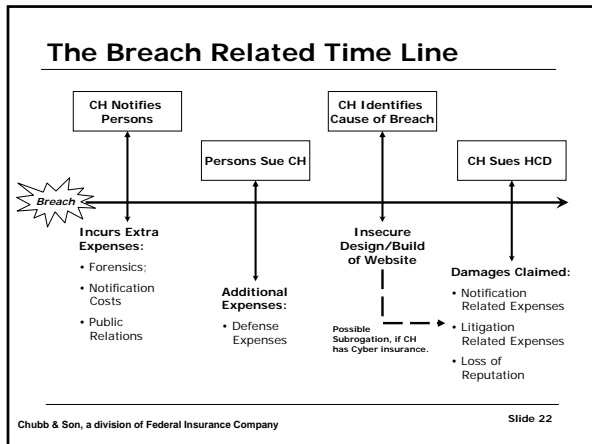


Immediately following the discovery of their breach, Caring Hands retains a Ace Investigators, a forensic investigator, to identify the cause of the breach.

Ace quickly discovers that Health Care Designs, the company CH hired to design and build their website, did not employ standard security measures when coding the website.

This made it easy for Myra to hack the site and access the patient data.

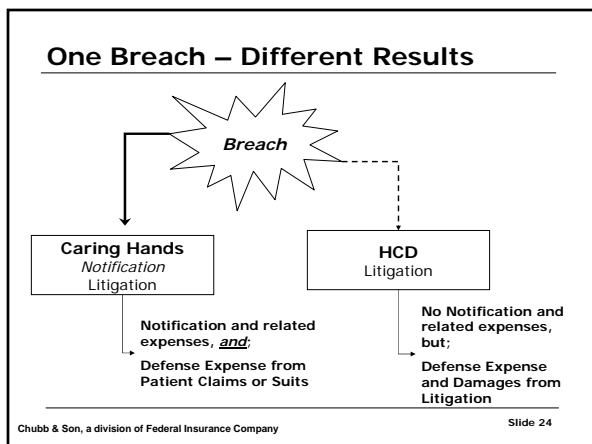
Caring Hands brings a suit against HCD to recoup their notification costs.



Damages – For An Organization

- Additional expenses incurred to carry out notification;
- Legal expenses to defend suit brought by patients;
- Loss of business resulting from injury to reputation;
- Loss of business resulting from diversion of personnel from primary responsibilities.

Chubb & Son, a division of Federal Insurance Company Slide 23



Different Insurance Responses

Caring Hands
Notification
Litigation

HCD
Litigation

Cyber Insurance

Notification Expenses
Public Relations Expenses
Forensic Expenses
Defense & Indemnity for
Claims or Suits

Technology E&O Insurance

Notification Expenses
Public Relations Expenses
Forensic Expenses
Defense & Indemnity for
Claims or Suits

Chubb & Son, a division of Federal Insurance Company

Slide 25

Another Data Breach



Caring Hands utilizes QuickCollect, Inc., a third party vendor, to process all their patient bills.

Accordingly, QuickCollect stores the names, addresses, credit card and other financial information of 75,000 existing and former CHH patients.

An employee of QuickCollect downloads the information to a laptop, which is subsequently stolen from his car.

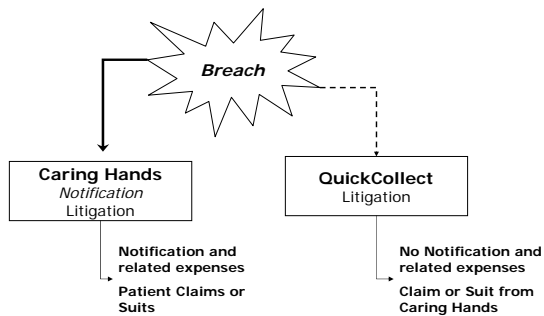
Following HIPAA rules, QuickCollect notifies CHH, who promptly notifies the patients.

What happens next?

Chubb & Son, a division of Federal Insurance Company

Slide 26

Different Breach – Same Results



Chubb & Son, a division of Federal Insurance Company

Slide 27

Again, Different Insurance Responses

Caring Hands
Notification
Litigation

QuickCollect
Litigation

Cyber Insurance

Notification Expenses
Public Relations Expenses
Forensic Expenses
Defense & Indemnity for
Claims or Suits from
Patients

Miscellaneous E&O Insurance(???)

Notification Expenses
Public Relations Expenses
Forensic Expenses
Defense & Indemnity for
Claims or Suits from

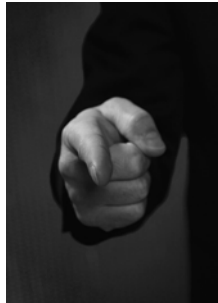
Chubb & Son, a division of Federal Insurance Company

Slide 28

So, Who Needs "Cyber" Insurance?

You Do, if you have:

1. A network that,
2. Stores "personal identifiable information" or "protected health information", and/or
3. Is connected to the Internet?



Chubb & Son, a division of Federal Insurance Company

Slide 29

More Specifically . . .

- Any organization that has the duty under a State or Federal law to notify individuals:
 - Generally, coverage for:
 - Notification expenses, other crisis management expenses, forensic expenses;
 - Litigation related expenses (defense & indemnity);
 - Defense expense of regulatory actions and, possibly, fines & penalties where allowed by law.
- Any organization that is processing or storing personal, confidential information for other organizations – and that does not carry Errors & Omissions insurance or whose E&O insurance may not respond to a "network security" type claim or suit.

Chubb & Son, a division of Federal Insurance Company

Slide 30

Well, Who May Rely On Just E&O?

- Any organization that only has the duty under a State or Federal law to notify the “owner” of the data in its care, custody or control; or
- Any organization that is creating or otherwise producing software or other technology products that could be used as a conduit for the fraudulent access to information.

When the E&O insurance policy covers a claim or suit alleging failure to “secure” data (including confidential information) or computer code.

One Last Scenario



Greg is going through the security check at Hartford Airport, but there are only 7 minutes before his flight is to depart.

His coat and shoes emerge from the x-ray machine, followed by his suitcase and briefcase.

As soon as he has his coat and shoes on, he grabs his bags and rushes to the gate, making it by only 30 seconds.

As the plane levels out at 22,000 feet, Greg realizes that he ran from Security without his laptop!

What will he do when he lands?

Are There Any -

QUESTIONS?
