


Cyber Risks Threats, Insurance & Risk Management Principles

George N. Allport
Vice President
Chubb Specialty Insurance



Legal Disclaimer

The views, information and content expressed herein are those of the author(s) and do not necessarily represent the views of any insurers of the Chubb Group of Insurance Companies.

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

Whether or not 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 2

Peppinger, Peppinger & Pink, LLP

Our Firm - History
Partners & Professionals
Practices & Expertise
News & Views
Publications & Reports



Personal Injury



Corporate & Tax



Wills & Probate



Criminal

Events At PP&P

- [Pep Peppinger MC's "10,000 Maniacs" Concert](#)
*Click Here To See Pep's Photos From The Concert
- Atlanta Office introduces "work from home" initiative
- The "Greening" of PP&P – Our Paper Reduction Initiative

News & Views

- [The Most Despicable People of 2009!](#)
- [Down & Out in Portland – Foreclosure Law & Defenses](#)
- [Will Helfer Help in Criminal Defense?](#)
- [Privacy – How Corporations Victimize Their Customers](#)



Search publications or employees

"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 PP&P's databases through their website.

She is able to access and download over the Internet names, addresses and Social Security numbers of 1,500 PP&P clients. She then sells the information to mobsters in Eastern Europe.

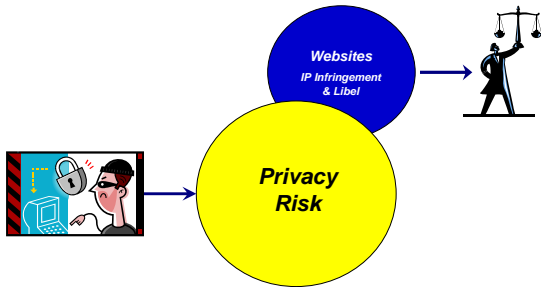
PP&P notifies their clients of the "breach" and some join a class action suit against PP&P.



Chubb & Son, a division of Federal Insurance Company

Slide 4

The Risks Today



Chubb & Son, a division of Federal Insurance Company

Slide 5

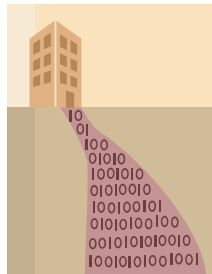
Data Breaches – Growing In Number!

Between January 10th, 2005 and February 9th, 2010

345,512,545

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

Source: Privacy Rights Clearinghouse
A Chronology of Data Breaches
Posted April 20, 2005
Updated February 9th, 2010
www.privacyrights.org



Chubb & Son, a division of Federal Insurance Company

Slide 6

So, Why Does PP&P 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, 43 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

Security Breach Statutes – Two Flavors



Acquisition Based Trigger

- Notification "triggered" by breach of the security of the system, as defined in statute.

Risk Based Trigger

- Notification "triggered" when there is a breach of the security of the system and determination of threat of identity theft or other fraud.

Chubb & Son, a division of Federal Insurance Company

Slide 12

Developing State Laws

- ❑ Massachusetts – Effective March 1, 2010
 - Requires encryption of confidential data when it is on a mobile device
 - Includes additional, robust security requirements for holders of personal information of Massachusetts residents
- ❑ Nevada – Effective January 1, 2010
 - Requires encryption of personal information held by any “data collector” doing business in Nevada when such data is transmitted or transported on a mobile device, off the collector’s premises.

Chubb & Son, a division of Federal Insurance Company

Slide 13

U.S. Federal Legislation



Chubb & Son, a division of Federal Insurance Company

Slide 14

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.

Chubb & Son, a division of Federal Insurance Company

Slide 15

HIPAA

Health Insurance Portability and Accountability Act of 1996

- Health care organizations must “maintain reasonable and appropriate technical and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information.
- Safeguards must apply to both transmission of information, as well as storage.

Chubb & Son, a division of Federal Insurance Company

Slide 16

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.

Chubb & Son, a division of Federal Insurance Company

Slide 17

Other Federal Regulators & Legislation

Security & Exchange Commission

- Sarbanes-Oxley Act

Federal Trade Commission

- Section 5 of The Federal Trade Commission Act prohibits unfair methods of competition and unfair or deceptive trade practices.

In August 1994, Congress amended the Act to provide that an act or practice is unfair if the injury it causes or is likely to cause to consumers is 1) substantial; 2) not outweighed by countervailing benefits to consumers or to competition; and 3) not reasonably avoidable by consumers themselves.”

<http://www.ftc.gov/opp/gpra/append1.shtm>

Chubb & Son, a division of Federal Insurance Company

Slide 18

Breach Related Expenses For PP&P



Notification

- Crafting letter or other notification
- Printing or design
- Mailing or other transmission

Public Relations

- Advertising & Press Releases
- Call Center Operations
- Other Services for Affected Persons:
 - Credit Monitoring

Forensics

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

Legal

- Response to Claims or Suits
- Payment of Judgments or Settlements

Breach Costs By Activity

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

Activity	Percent	Dollar
Investigation & Forensics	8%	\$16
Audit & Consulting Services	12%	\$24
Outbound Contact	6%	\$12
Inbound Contact	5%	\$10
Public Relations/Communications	1%	\$2
Legal Services - Defense	14%	\$29
Legal Services - Compliance	2%	\$4
Free or Discounted Services	1%	\$2
Identity Protection Services	2%	\$4
Lost Customer Business	40%	\$82
Customer Acquisition Cost	9%	\$18
Total	100%	\$204

Damages – An Obstacle For Plaintiffs

- ❑ 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



Traditional Insurance Coverage?

ISO Commercial Property?

Electronic Data Extension only addresses loss or damage to data which has been *destroyed or corrupted* by a covered cause of loss.

Commercial Crime Form?

No coverage due to the Definition of "Other Property" and the Exclusion of "Indirect Loss".

General Liability Policy?

Addresses only physical injury to persons or tangible property, as well as the Insured's publication of material that violates a person's right to privacy.

Professional Liability Policy?

May be limited by the description of "Professional Services" or by Exclusions for "Invasion of Privacy".

Chubb & Son, a division of Federal Insurance Company

Slide 22

More Schemes, Scams and Crimes



Chubb & Son, a division of Federal Insurance Company

Slide 23

"A New Twist"

On a "black hat" website, Myra learns about a vulnerability in the "25Hour Day" legal billing software used by PP&P.

Exploiting the vulnerability, she accesses and downloads over the Internet names, addresses and Social Security numbers of 1,500 PP&P clients. She then sells the information to mobsters in Eastern Europe.

PP&P notifies their clients of the "breach" and some join a class action suit against PP&P.

Myra then encrypts all the data on PP&P's servers.

PP&P's system is useless and PP&P can't process work for their clients.

She offers to sell PP&P the encryption key for \$1.5 Million.



Chubb & Son, a division of Federal Insurance Company

Slide 24

More Risks Today

Chubb & Son, a division of Federal Insurance Company Slide 25

Additional Expenses For PP&P

<p>Breach Notification Expenses</p> <ul style="list-style-type: none"> ➢ Mailings ➢ Public Relations ➢ Forensics 	<p>Business Interruption & Extra Expense</p> <ul style="list-style-type: none"> ➢ Extra Expenses Incurred to Continue Operations ➢ Loss of Profit Due to Impairment of Operations 	<p>Extortion Threat</p> <ul style="list-style-type: none"> ➢ Ransom Payment ➢ Negotiation Expenses ➢ Legal and Other Related Expenses 	<p>Legal</p> <ul style="list-style-type: none"> ➢ Response to Claims or Suits Related to Data Breach ➢ Response to Claims or Suits for Impairment of Computer Services
--	--	---	---

Chubb & Son, a division of Federal Insurance Company Slide 26

The "Perfect Storm"

<p style="text-align: center; background-color: #0056b3; color: white; padding: 2px;">First Party</p> <p><u>Loss of Private Data</u></p> <ul style="list-style-type: none"> • Notification Costs • Publicity Costs • Crisis Management Expenses <p><u>Business Continuity Expense</u></p> <ul style="list-style-type: none"> • Extra Expenses to continue operations • Business Income loss <p><u>Cyber Extortion</u></p> <ul style="list-style-type: none"> • Ransom Payment • Other Expenses 	<p style="text-align: center; background-color: #c00000; color: white; padding: 2px;">Third Party</p> <p><u>Client Suits - Privacy</u></p> <ul style="list-style-type: none"> • Suits from clients alleging negligence in protecting information and other causes of action <p><u>Client Suits - Denial of Service</u></p> <ul style="list-style-type: none"> • Suits from clients alleging negligence in protecting the network against denial of service
--	---

Chubb & Son, a division of Federal Insurance Company Slide 27

Don't Think That This Can Happen?

The Bloomberg Scenario

4/19/07 12:20:00

SECURITY NET
By Alex Salameh



Cyber-Extortion: When Data Is Held Hostage

Here's an issue facing more and more e-businesses - malicious hackers who demand a payoff to keep their security breaches secret

Under most circumstances, a business decision involving \$200,000 wouldn't be important enough to require a personal appearance from the CEO of a \$2 billion corporation. Yet when a special trip to London from New York, 600 miles from Michael Bloomberg made such a trip Aug. 13. And he did it to prove that cyber-extortion will not go unpunished at his company.

Bloomberg went to meet with her Krazzies named Clay Zetter, 37, and Igor Karmali, 37, who were allegedly demanding \$200,000 in "ransoming" fees. For this, they would reveal how they had allegedly compromised the Byzantine Bloomberg computer systems, an exploit the Krazzies allegedly proved by e-mailing Bloomberg the photograph from his own corporate ID badge.

With thousands of financial institutions and other customers trading billions of dollars daily in stocks and bonds based on information from Bloomberg terminals, the threat of a hacked system could have proven catastrophic for both the media company and its Wall Street customers.

Chubb & Son, a division of Federal Insurance Company

Slide 28

The Boston Globe

By Kelly Olsen

Associated Press Writer / July 8, 2009

SEOUL, South Korea—North Korea, which has been firing missiles and spewing threats against the United States, has been identified by South Korea's main spy agency as a suspect in the cyber attacks targeting government and other Web sites in the U.S. and South Korea.

The attacks began paralyzing Web sites in the U.S. over the July 4 U.S. Independence Day holiday weekend and in South Korea on Tuesday and Wednesday. A South Korean computer security company said that another wave of cyber attacks was expected in South Korea later Thursday.

Chubb & Son, a division of Federal Insurance Company

Slide 29

"Phishing" E-Mail Example

Bank of America Higher Standards



Online Banking Alert

Need additional
info on this message
account
infected with
virus?

Click here

Restore Your Online Access

Because of unusual number of invalid login attempts on your account, we had to believe that, there might be some security problem on your account. So we have decided to put an extra verification process to ensure your identity and your account security. Please click on [sign in to Online Banking](#) to continue to the verification process and ensure your account security. It is all about your security. Thank you, and visit the customer service section.

Chubb & Son, a division of Federal Insurance Company

Slide 30

What's "Social Engineering"?



Spear Phishing



An employee in Zircon Manufacturing's treasury department receives an e-mail, purportedly from the client liaison at Zircon's bank, saying that some of the bank's files have been corrupted and asking the employee to send the client representative Zircon's correct account numbers and passwords.

The employee complies.

Over the following weekend, \$500,000 is fraudulently transferred out of Zircon's account.

Chubb & Son, a division of Federal Insurance Company

Slide 31

Cyber Policies -



What To Look For

Chubb & Son, a division of Federal Insurance Company

Slide 32

Loss Events – Third and/or First Party?



Third Party Loss:

- ❑ Defense Expenses & Damages
 - > Notification Expenses
 - > Other Crisis Management Expenses

First Party Loss:

- ❑ Extra Expense & Business Income Loss from Denial of Service
- ❑ Extortion Related Loss
- ❑ Corruption or Destruction of Data

Chubb & Son, a division of Federal Insurance Company

Slide 33

Does the Policy Address -

- Access to information other than by over the Internet?
- Access to information by an employee?
- Access to information residing on an "outsourced" system – anywhere?
- Access to information in "non-electronic" form?
- Negligent release of information?



Chubb & Son, a division of Federal Insurance Company

Slide 34

What Information Assets Are Covered?

Personal Identifiable Information (PII)

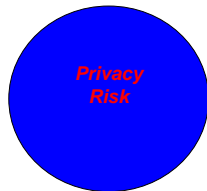
- Customers, Employees, Others?

Personal Health Information (PHI)

Business Property:

- Customer Lists (non-PII)
- Financial Information
- Marketing & Operational Information

Trade Secrets



Chubb & Son, a division of Federal Insurance Company

Slide 35

Crisis Management Considerations -

• Notification Expenses

*When required by law or on a voluntary basis?
Insurer pre-approval required?*

• Credit Monitoring Expenses

For a stipulated period of time and/or under specified circumstances?

• Crisis Management Expenses (including legal analysis expense)

Including expenses related to legal analysis, as well as public relations?

Chubb & Son, a division of Federal Insurance Company

Slide 36

Watch The Exclusions!



- ❑ Some policies exclude coverage for "claims" related to the Insured's *failure to maintain or upgrade their security!*
- ❑ Some policies exclude coverage for "claims" alleging fraudulent or malicious acts by *employees!*
- ❑ Some policies exclude certain operations of the Insured, or may not cover various types of computer or peripheral device!

Chubb & Son, a division of Federal Insurance Company

Slide 37

Other Policy Considerations

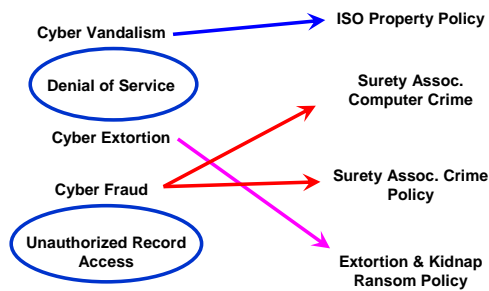


- ❑ Duty to Defend - Selection of Counsel?
- ❑ Defense of Regulatory Suits or Actions?
- ❑ Coverage for Fines & Penalties?
 - If so, what's the definition or interpretation?
- ❑ Warranty, Retro Date, Prior Acts?
- ❑ Other Insurance Clause?

Chubb & Son, a division of Federal Insurance Company

Slide 38

Common First Party "Gaps"



Chubb & Son, a division of Federal Insurance Company

Slide 39

Risk Management & Security Practices



Chubb & Son, a division of Federal Insurance Company

Slide 40

Three Branches of Security

Managerial



Security Awareness
Security Planning & Testing
Auditing & Controls
Crisis Management

Technical



Network Design
Network Protection
Vulnerability Testing
Vulnerability Remediation
Application Development,
internal & external

Operational



Physical Security of Premises
Mobile Devices
Vendor Management

Chubb & Son, a division of Federal Insurance Company

Slide 41

So, You Still Need Insurance!

The Cyber Fortress May Not Defend Against:

- Previously Unknown Intrusion Techniques (*Zero Day Exploits*):
 - IBM estimates that only 5.48% of existing vulnerabilities were made known to the public in 2006
- Your "Rogue" Employees or Your Vendors' "Rogue" Employees;
 - Confidential Information may be Bought from Employees
 - Disgruntled Employees may Damage or Destroy Data or Networks
- Negligence in Protecting Your Data, or Safeguarding Your Data .
 - Misdirected e-mails or shipments of electronic records;
 - Poor safeguarding of laptops;
 - Social engineering

Chubb & Son, a division of Federal Insurance Company

Slide 42

Are There Any -

QUESTIONS?

Chubb & Son, a division of Federal Insurance Company

Slide 43
