Network Security & Privacy Risk

Are You Prepared?

Presented By:
Wells Fargo Insurance
Scott Lockman

Together we'll go far

Agenda

- Statistics
- Recent Headlines & Prominent Examples
- Costs by Data Type, Breach and Cause of Loss
- The Grander Scheme of Things
- Legal Issues and The Regulatory Environment
- The Plaintiff Bar's push…
- Are You at Risk?
- Incident Response
- Network Security & Privacy GAP Analysis
- What is a Privacy/Security Breach?
- Third Party Claim Allegations
- High Hazard Industry Classes
- What Can Be Covered …?
- Enterprise Privacy Coverage
- Vendor Management & Requirements
- The Primary Markets
- Marketing & Underwriting Process
- eRisk Hub
- How Does a CFO Rank Risk?

Did You Know?

2011 Cost of Data Breach Study: United States*

- The average cost per compromised record declined to $194, compared to $214 in 2010 and $204 in 2009.
- Average expense to an organization declined to $5.5 M from $7.2M in 2010, in direct and indirect costs, which includes the cost of notifying victims and maintaining information hot lines as well as legal, investigative and administrative expenses.
- More customers remain loyal following a data breach. Certain industries are susceptible to customer churn, which causes data breach expenses to be higher.
- Negligent insiders and malicious attacks are the main causes of data breaches. 39% of organizations say that negligence was the root cause of the data breach.
- Malicious attacks accounted for more than a third of the total breaches reported in the study. They are the most costly breaches.
- Lost business costs declined sharply from $4.5M in 2010 to $3.01M in 2011. These costs refer to abnormal turnover of customers, reputation losses and diminished goodwill.

* **Ponemon Institute© Research Report - 2011**

But wait, there's more. . .

- Certain organizational factors reduce the overall cost. If the organization has a CISO with overall responsibility for enterprise data protection, the average cost of a breach can be reduced as much as $80 per compromised record.
- Outside consultants assisting with the breach response can save as much as $41 per record, which can provide a significant positive financial result.
- Organizations that had their first data breach spent on average $37 more per record.
- Organizations that responded or notified customers too quickly without a thorough assessment of the breach paid an average of $33 more per data breach.
- Detection and escalation costs declined but notification costs increased. The costs to notify victims of a breach increased in the 2011 study from approximately $510,000 to $560,000. A key factor is the increase in laws and regulations governing data breach notification.

Recent Headlines & Prominent Examples

Sutter Health
October 2011

Approx. 4M records were compromised as a result of a stolen laptop. $1B class action was filed against **Sutter** in November 2011. Total damages TBD.

Sony Corporation
April 2011

Approx. 70M records compromised and estimated cost in the billions.

TJX
2007

Approx. 94M customer credit/ debit cards compromised. Total cost over $250M.

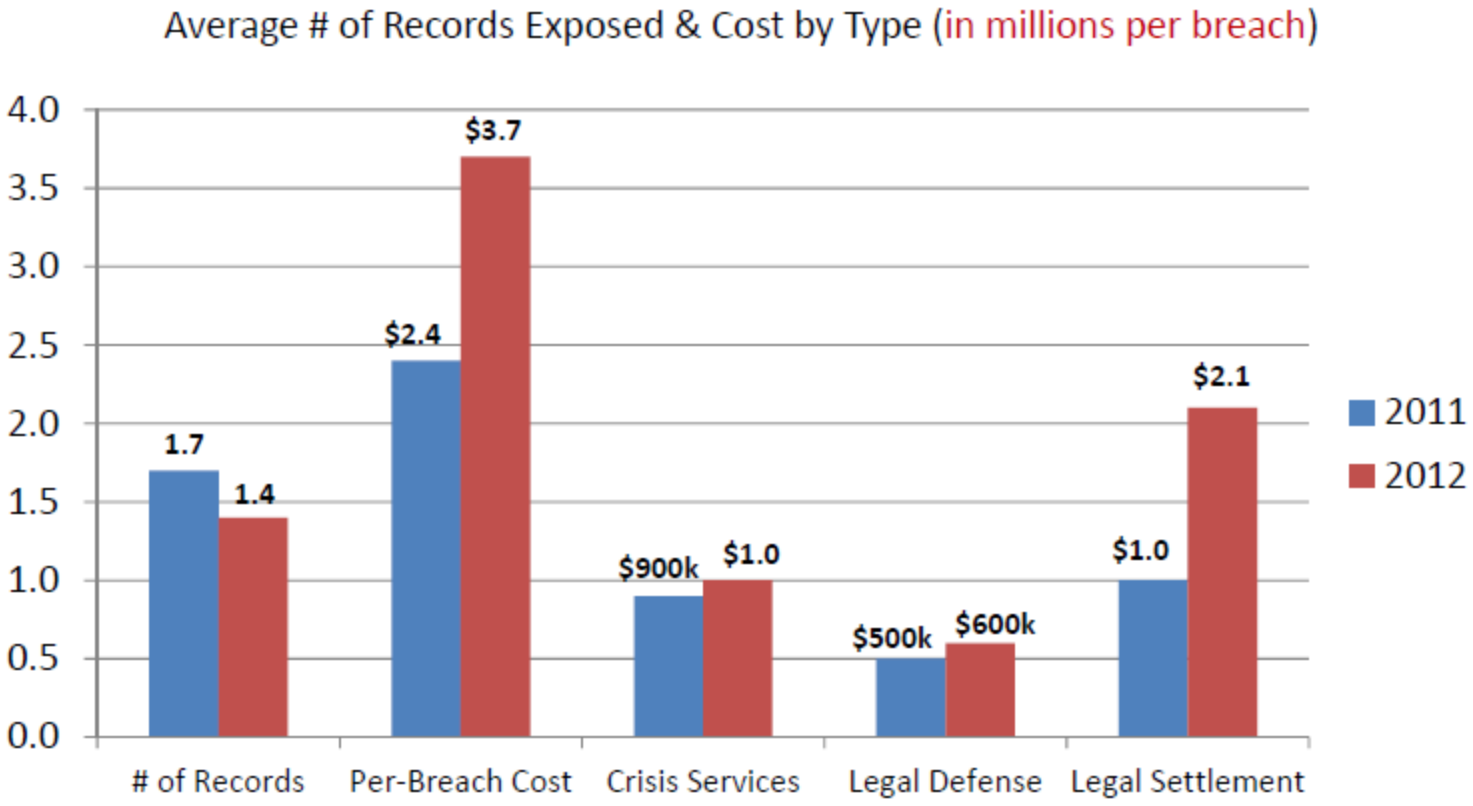
Epsilon
April 2011

The email marketing firm notified over 2,500 customers of a data breach potentially compromising 40 billion email addresses. Significant data breach expenses incurred, and damage to reputation.

Heartland Payment Solutions
November 2008

Approx. 130M customer credit/ debit cards compromised. Companion D&O suit filed. Total cost incurred approximately $140M including settlements with VISA.

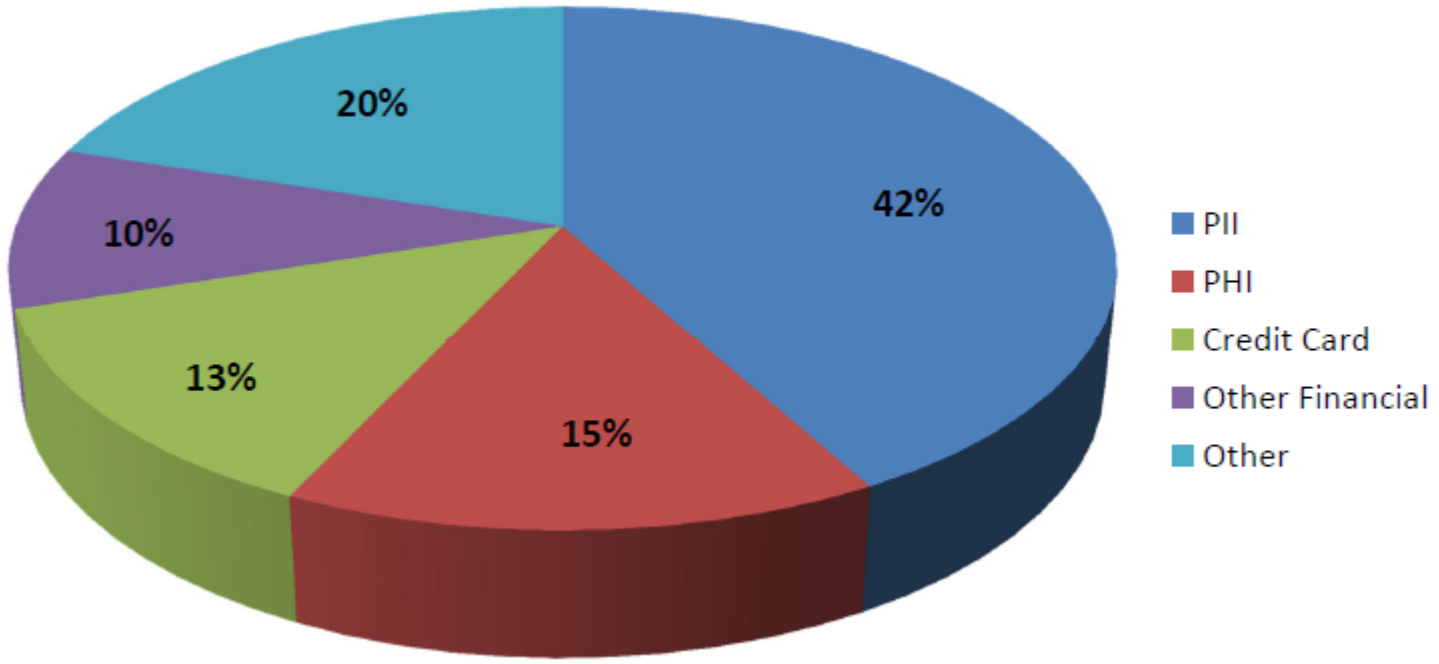
Comparing 2012 & 2011 Findings



** Cyber Liability & Data Breach Insurance Claims - NetDilligence® June 2012*

Percentage of Breaches by Data Type

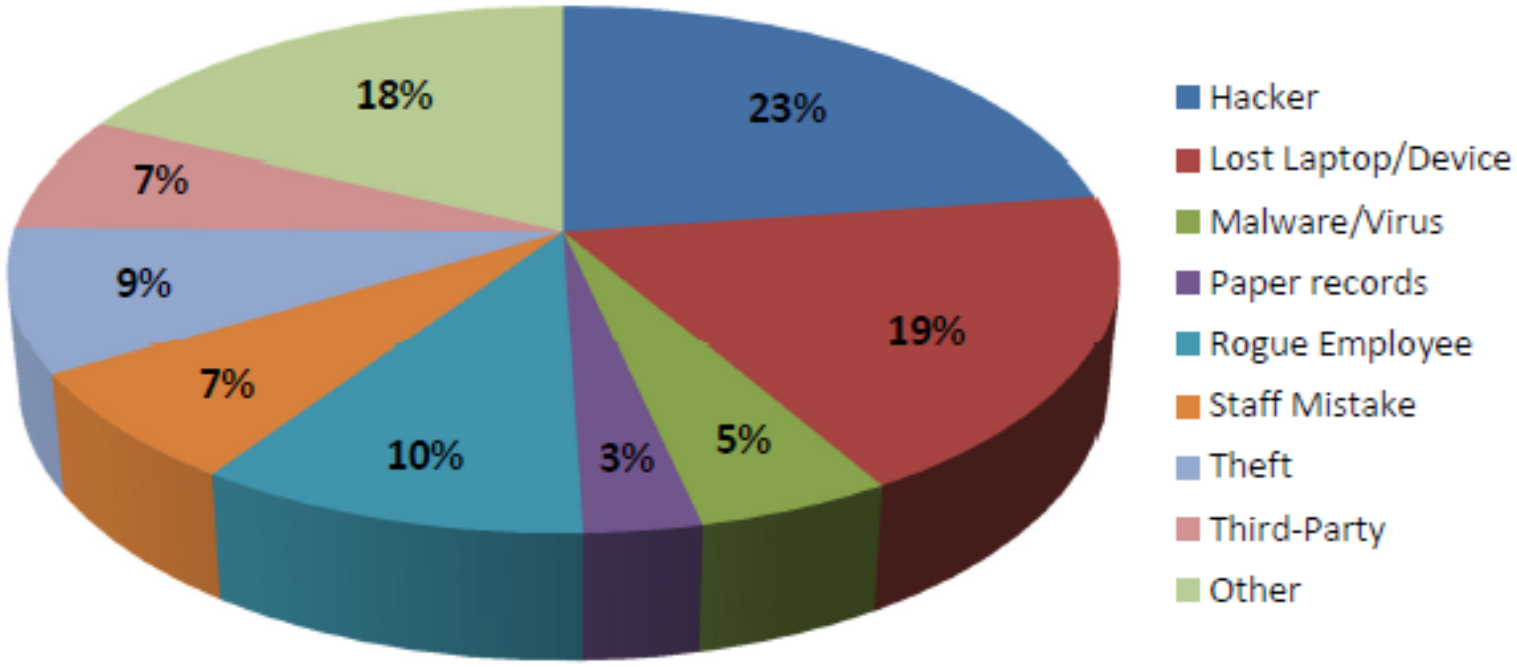
Third-Party Liability



** Cyber Liability & Data Breach Insurance Claims - NetDilligence® June 2012*

Percentage of Breaches by Cause of Loss

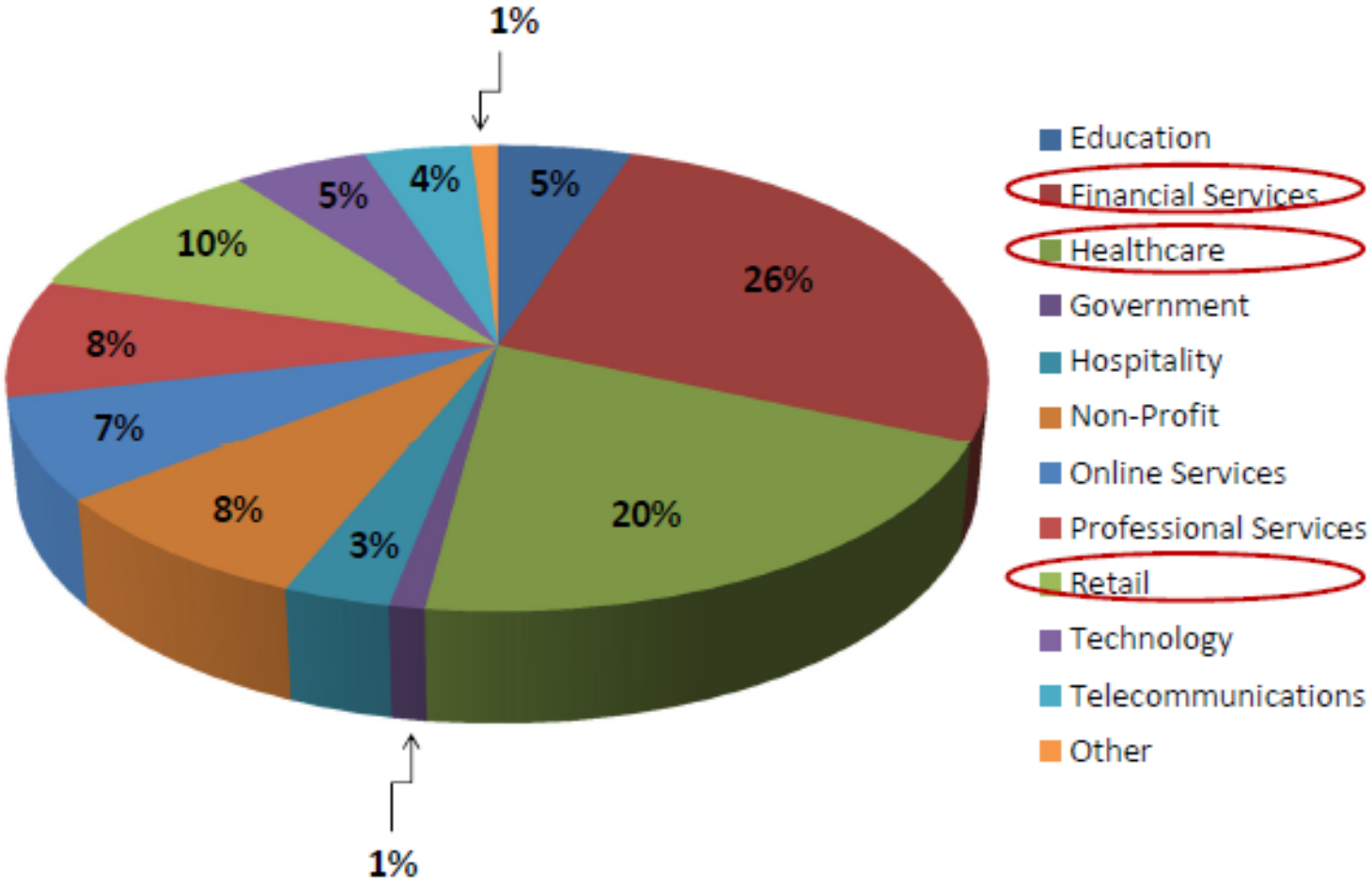
Third-Party Liability



** Cyber Liability & Data Breach Insurance Claims - NetDilligence® June 2012*

Percentage of Breaches by Business Sector

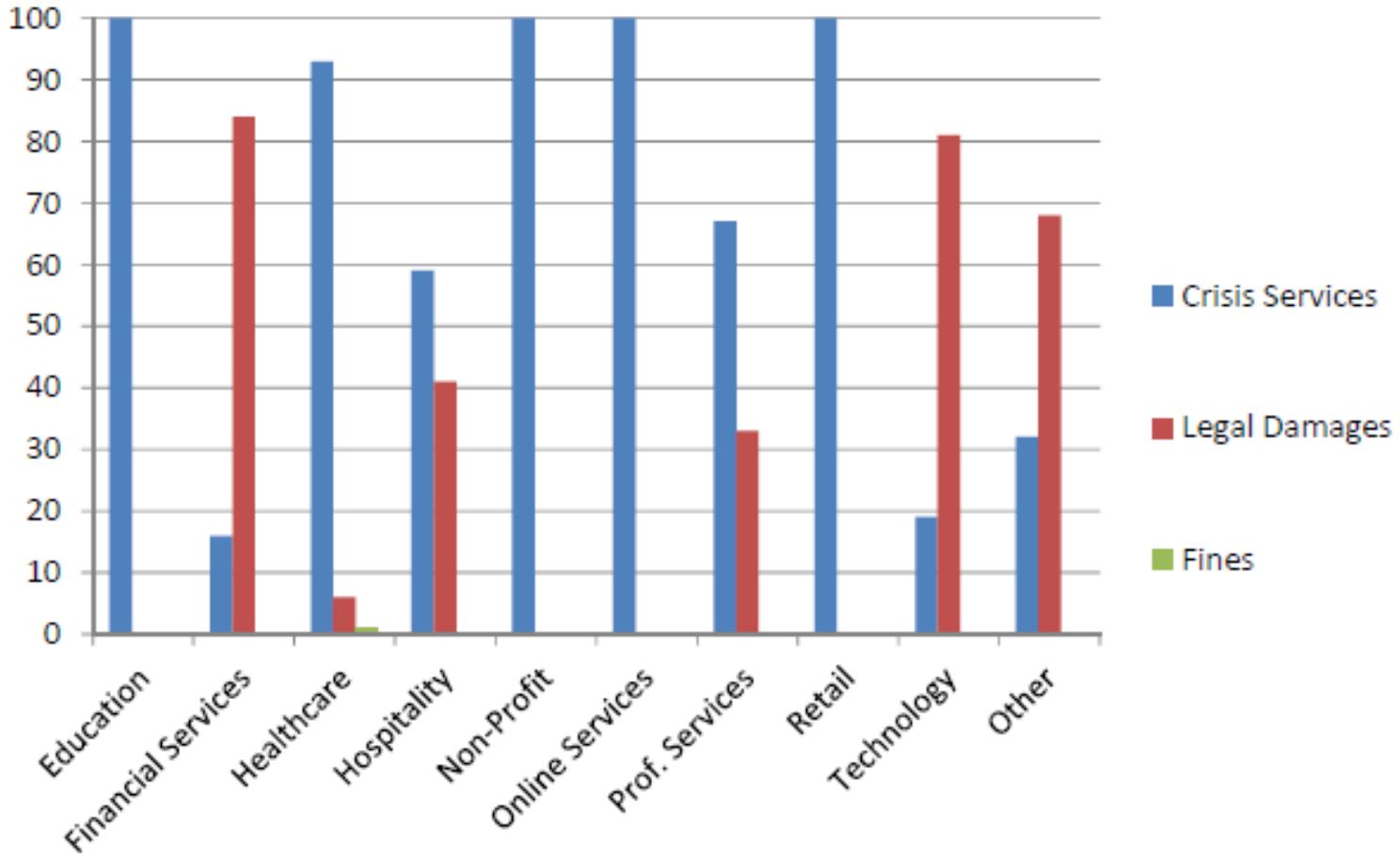
Third-Party Liability



** Cyber Liability & Data Breach Insurance Claims - NetDilligence® June 2012*

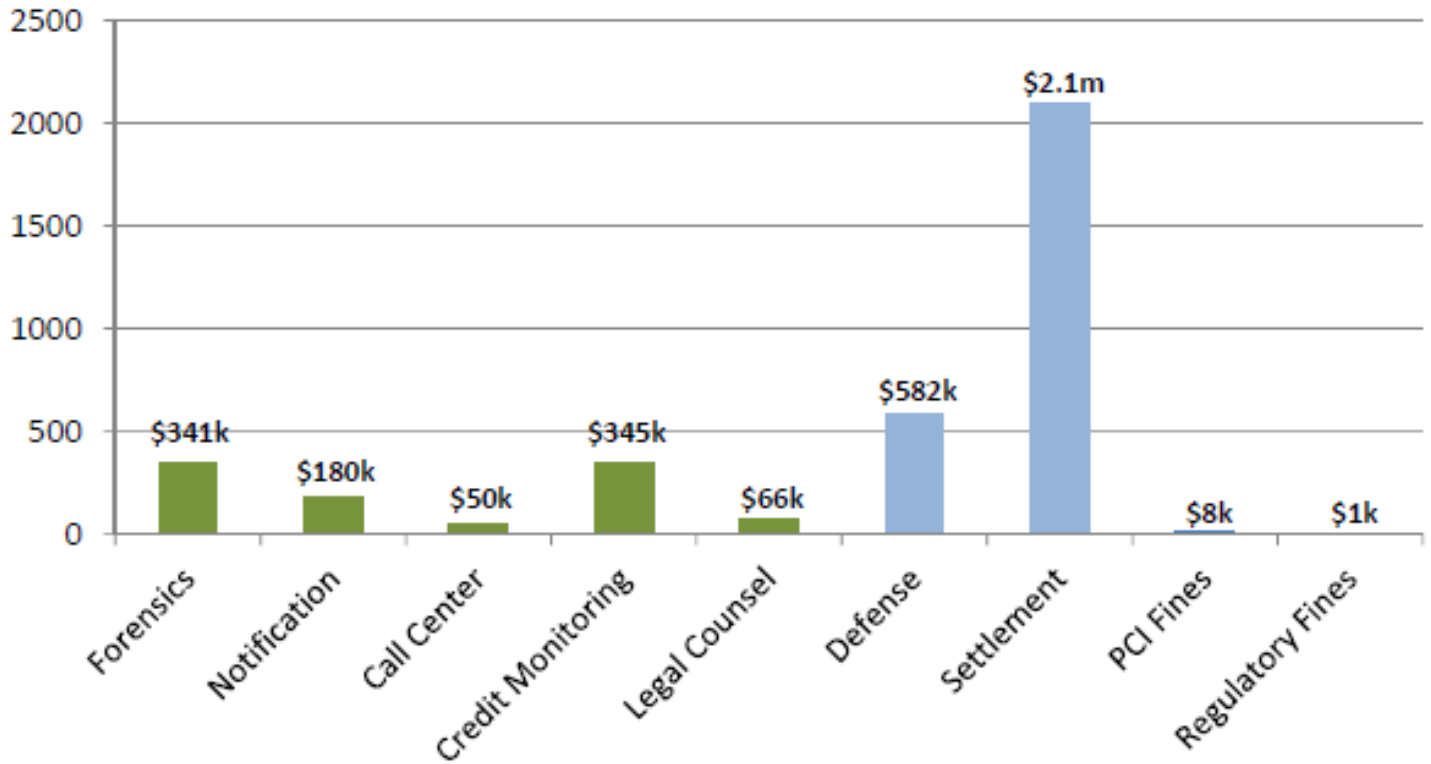
Percentage of Costs by Business Sector

Third-Party Liability



** Cyber Liability & Data Breach Insurance Claims - NetDilligence® June 2012*

Average Cost per Breach
Third-Party Liability



** Cyber Liability & Data Breach Insurance Claims - NetDilligence® June 2012*

The Grander Scheme of Things…

Not only can a security event have a severely negative impact on your reputation but it could…….

- Adversely impact your debt covenants
- Impair cash flow as funds are redirected to respond to the costs associated with the security event
- Affect stock price
- Redirect the focus of key employees from their daily jobs to the management of an event (it has been estimated that the "people-hour" cost for a breach is $30 per record breached)
- Cause an exodus of customers
- Create vulnerabilities that can be played upon by your competitors

Legal Issues & The Regulatory Environment

Legislation has now imposed affirmative duties on companies as to how they handle data, principally client/customer information:

- **Gramm Leach-Bliley Act:** Requires financial institutions to safeguard customers' records and information against unauthorized access. Imposes major privacy and security requirements on financial services companies.
- **Health Insurance Portability and Accountability Act (HIPAA):** Healthcare organizations required to safeguard individually identifiable health information. Imposes penalties on organizations that violate HIPAA (further amended by the HITECH Act).
- **California SB1386:** A California law requiring companies to notify their CA customers and employees of computer security breaches. The law applies to any business that stores customer and employee information electronically even if the company is not based in the Golden State.
- **Privacy Breach Notification Laws**: Spreading of California SB 1386; adopted by 46 states as of June 2011. Duty to notify customers where consumer/customer information has been compromised (electronic or non-electronic means, state legislation varies).
- **Massachusetts Privacy Law 201 CMR 17.00**: This law is the first state law to require specific technology when protecting personal information. If you do business with residents in MA or have employees that reside in MA, compliance is mandatory by March 1, 2010.

More Legal Issues & the Regulatory Environment

- **FACTA (Fair and Accurate Credit Transactions Act):** Prohibits businesses from printing more than 5 digits of any customer's credit card number or card expiration date on any receipt issued at a point of sale. For machines in use before 1/1/05, the merchant has 3 years to comply. For machines in use after 1/1/05, the merchant has one year to comply.
- **Red Flag Rules:** Established by FACTA, requires financial institutions or creditors to develop and implement an Identity Theft Prevention Program in connection with both new and existing accounts. The program must include reasonable policies and procedures for detecting, preventing and mitigating identity theft.
- **Federal HITECH Act** – health plans, health care providers and health care clearinghouses (i.e.. Covered entities), among other things, must review and update their business associate agreements, as well as their privacy and security policies and procedures. Requires that any data breach event exceeding 500 records be reported to the Department of Health and Human Services.
- **PCI Security Standards:** The standards globally govern all merchants and organizations that store, process or transmit cardholder data. PCI security standards are technical and operational requirements set by the Payment Card Industry Security Standards Council.

The Plaintiff Bar's push for their day in court

While the courts have been reluctant to push these suits through to class status, we have been seeing some movement in favor of the plaintiff's bar. For example:

- **Krottner v. Starbucks Corp.** – The Ninth Circuit Court of appeals found that the possibility of identity theft was " a credible threat of harm" sufficient to meet the injury-in-fact requirements of standing. (The court also affirmed the plaintiffs did not have a cause of action for negligence or contract liability under Washington law however the court has allowed the case to move forward).

- **RockYou** – The court concluded that the plaintiff has sufficiently alleged a general basis for harm by alleging that the breach of his PII has caused him to lose some ascertainable but unidentified value and or property right inherent in the PII. Therefore, the court has allowed the case to move forward.

- **Anderson v. Hannaford Brothers Co.** - Interesting decision as the facts in this case are different from many of the potential class actions we are seeing in two respects: 1) the plaintiffs had demonstrated in their pleadings that hackers intended to steal the customers information; and 2) plaintiff's actually suffered damages in that their personal information was used to their detriment and they incurred costs to mitigate the damage.

- **Paul v. Providence Health System Oregon, Katz v. Pershing, LLC–** rulings stated that a data breach alone does not constitute injury giving rise to recoverable damages. There must be use of the information stemming from the data breach. In these cases, the plaintiff's bar was not successful.

Are You at Risk?

Ask Your Team:

- Has your organization ever experienced a data breach or system attack event?
- Does your organization collect, store or transmit any personal, financial or health data?
- Do you have a solid incident response plan in place?
- Do you outsource any part of computer network operations to a third-party service provider?
- Do you use outside contractors to manage your data or network in any way?
- Do you partner with businesses and does this alliance involve the sharing or handling of their data (or your data) or do your systems connect/touch their systems?
- Does your posted Privacy Policy actually align with your internal data management practices?
- Has your organization had a recent cyber risk assessment of security/ privacy practices to ensure that they are reasonable and prudent and measure up with your peers?

Incident Response

When a data breach strikes, you must respond quickly and address customer concerns.

- ✓ Assemble your core incident response tea
- ✓ Confirm your priorities
- ✓ Contain, Fix, Restore
- ✓ Engage Pre-selected External Resources
- ✓ Conduct an incident risk assessment
- ✓ Notify customers and regulators
- ✓ Set up a call center
- ✓ Know federal and state requirements
- ✓ Report the breach to federal and state agencies
- ✓ Be prepared for an investigation

***Data provided by ID Experts www2.idexpertscorp.com/resources**

Network Security & Privacy GAP Analysis

	Property	General Liability	Crime	K&R	E&O	Network Security & Privacy
1st Party Privacy/Network Risks						
Physical Damage to data only	❑	☒	❑	☒	❑	❑
Virus/Hacker damage to data only	❑	☒	☒	☒	❑	☑
DOS (Denial Of Service) Attack	❑	☒	☒	☒	❑	☑
BI Loss from security event	❑	☒	☒	☒	☒	☑
Extortion or Threat	☒	☒	☒	☑	☒	☑
Employee Sabotage of data only	☒	☒	❑	☒	❑	☑
3rd Party Privacy/Network Risks						
Theft/Disclosure of private information	☒	❑	❑	☒	❑	☑
Confidential Corporate information breach	☒	❑	☒	☒	❑	☑
Technology E&O	☒	☒	☒	☒	☑	☒
Media Liability (electronic content)	☒	❑	☒	☒	❑	❑
Privacy Breach expense/notification	☒	☒	☒	☒	☒	❑
Damage to 3rd Party's data only	☒	❑	❑	☒	❑	☑
Regulatory Privacy Defense / Fines	☒	☒	☒	☒	☒	❑
Virus/Malicious code transmission	☒	❑	☒	☒	❑	☑

☒ - No Coverage ❑ - Possible Coverage ☑ - Coverage

What is a Privacy Breach / a Security Breach?

A ***privacy breach*** is the theft, loss or unauthorized disclosure of personally identifiable non-public information (PII) or third party corporate confidential information that is in the care, custody or control of the organization or an agent or independent contractor that is handling, processing, sorting or transferring such information on behalf of the Organization.

Exposures as a result of a privacy breach can also include the organization's failure to timely disclose an incident (or reasonably suspected incident), a failure to comply with an organization's privacy policy and the failure to administer an identity theft program (i.e.. MA privacy law)

A ***computer security breach*** is the inability of a third party, who is authorized to do so, to gain access to an organization's systems or services; the failure to prevent unauthorized access to an organization's computer systems that results in a destruction, deletion or corruption of data, theft of data; a denial of service attack against an organization's internet sites or computer systems; or the failure to prevent transmission of malicious code from an organization's systems to a third party computers and/or systems.

Third Party Claim Allegations Can Include:

- Failure to implement and maintain reasonable security procedures
- Failure to timely notify
- Negligence
- Unfair or deceptive business practices
- Failure to safeguard personally identifiable information in your care, custody or control and therefore violating a customer's right to privacy
- Breach of contract
- Breach of fiduciary duty
- Misrepresentation
- Violation of the Fair Credit Reporting Act

High Hazard Industry Classes

- Healthcare
- Financial Institutions
- Retail
- e-Commerce companies
- Schools, Colleges and Universities
- Information / Data Services companies
- Credit Card Processors
- Public Entities

What Can Be Covered Under a Network Security & Privacy Policy?

- **Breach of Security:** Your liability to third parties arising out of a failure of your network security that results in a computer attack. Such failure can be caused by unauthorized access or use, transmission of a computer virus or a denial of service attack.
- **Invasion of Privacy:** Your liability arising from disclosure and release of confidential or personally identifiable information stored on your computer system caused by a failure of your network security.
- **Enterprise Privacy:** Your liability arising from any breach of privacy including violations of HIPAA, GLB or any state, federal or foreign privacy protection law (including regulatory defense expenses, notification expenses, credit monitoring, crisis management expenses)
- **Identity Theft:** Your liability arising from theft of personal information of your employees, customers or clients.
- **Cyber Extortion:** Protection against threats or demands made against you involving your computer network.
- **Internet Media:** Defamation, Libel and Slander/Personal Injury – Liability arising out of the content disseminated on your Internet site; includes intellectual property infringement exposures
- **Business Interruption:** Business Interruption losses sustained by you arising from the interruption or suspension of your computer network, due to failure of security (including extra expenses)
- **Data Asset Coverage:** Information asset protection for you for property losses involving data, computer systems and information assets arising from a computer attack.

Enterprise Privacy Coverage

- **Non-network Privacy Breaches:** What happens if a breach, which exposes confidential information, does not arise out of a failure of security of your computer system? i.e.. paper, PDA's, lost data tapes.
- **Accountability For Outside Vendors:** Your liability arising from others working on your behalf (those which you are legally responsible for).
- **Employee Privacy Exposure:** What happens if a breach causes your employees' confidential information to be compromised?
- **Regulatory Defense Expenses:** Defense costs involved with a regulatory proceeding, a request for information, demand, suit or civil investigation by or on behalf of a government agency arising from allegations of violation of a privacy regulation (may include coverage for fines & penalties and related consumer redress fund expenses)
- **Notification Expenses:** Costs to notify your customers/clients of security or privacy breaches. Most insurers will provide a sub-limit of coverage to assist with these expenses.
- **Credit Monitoring Expenses:** Costs to provide your customers/clients with credit monitoring services as a result of privacy violation, if you have the duty to provide.
- **Crisis Management Expenses:** Reasonable and necessary expenses incurred by you and approved by the Insurer in retaining the services of a public relations firm, law firm for advertising or related communications to assist with mitigating harm to your reputation.

* Regulatory Expenses, Notification Expenses, Credit Monitoring and other Crisis Management Expenses are generally offered on a sub-limited basis and varies by carrier.

Vendor Management & Requirements

Due Diligence on Vendors is Key – Secondary is Insurance Requirements

IT/Software Companies

- Request Tech E&O to include network security/privacy coverage
- Some Tech E&O policies have security/privacy exclusions

Other Business Services – Payroll, Auditors

- Request appropriate E&O coverage to include network security/privacy

Credit Card Processors/Acquiring Banks

- Request Network Security/Privacy Coverage

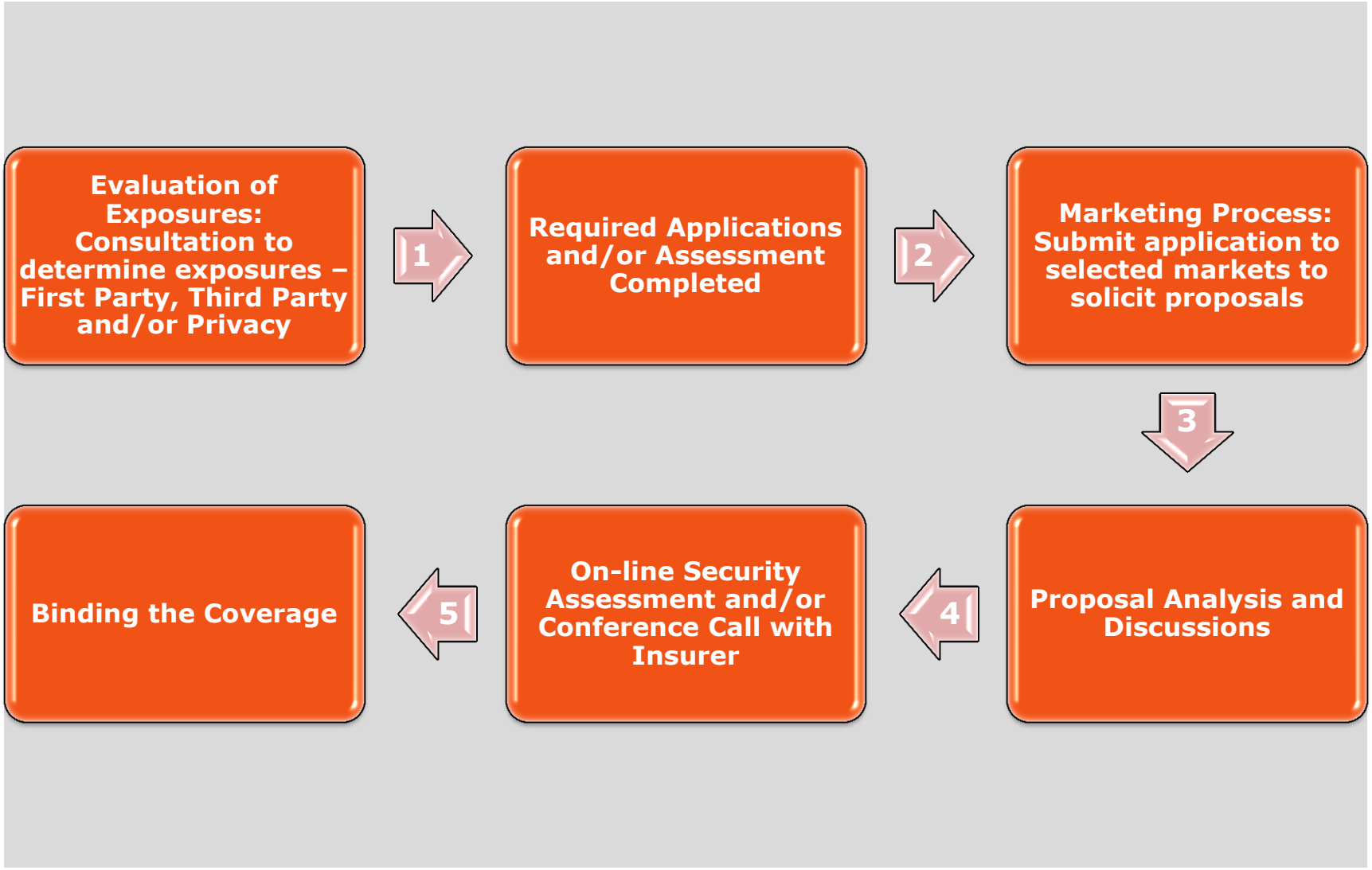
Other Vendors that interact with your systems or sensitive information, or handle information on your behalf

- Request Network Security/Privacy Coverage

The Primary Retail Markets

Markets	Best Rating
ACE USA	"A+" XV
AWAC (fka Darwin Group)	"A" XV
Arch	"A" XV
Axis	"A" XV
Beazley USA	"A" VIII
AIG (fka Chartis)	"A" XV
Chubb Group	"A++" XV
CNA	"A" XV
Digital Risk Managers (MGA writing on Lloyds paper – Brit, Kiln, Barbican)	"A" XV
Hartford	"A" XV
Hiscox USA	"A" VIII
Ironshore	"A-" XIII
Liberty	"A" XV
London Markets (Beazley, Hiscox, Brit, Kiln, ACE, CFC, etc)	"A" XV
One Beacon	"A" XV
Philadelphia	"A" XV
Travelers	"A+" XV
Zurich North America	"A" XV
XL	"A" XV

Marketing & Underwriting Process



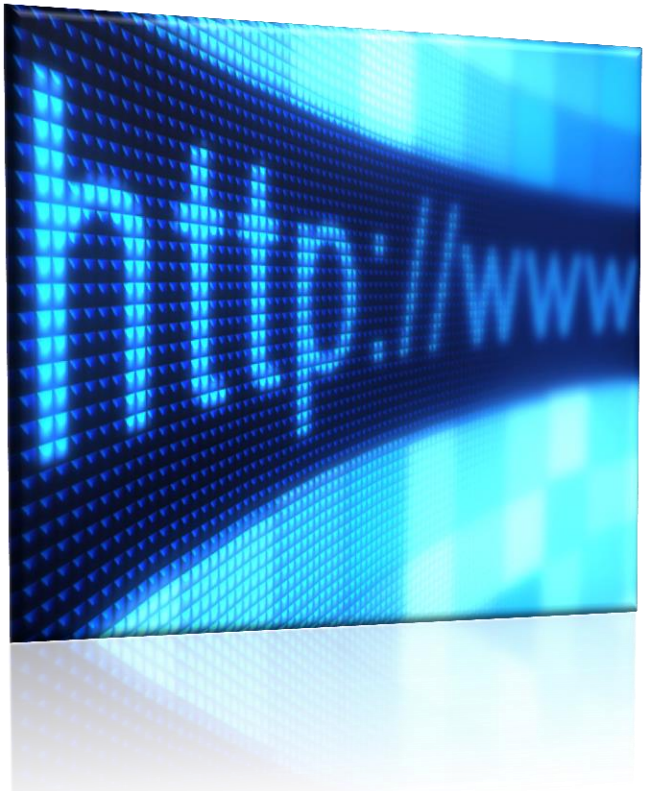
Key features of the eRisk Hub

- **Breach Coach™** – Our Breach Coach service, staffed by attorneys who are certified privacy professionals, provides immediate triage assistance in the event of a breach.

- **News Center** – The news center keeps you up to date with cyber risk stories, security and compliance blogs, security news, risk management events, and helpful industry links.

- **Learning Center** – The learning center contains best-practices articles and white papers written by leading technical and legal professionals on compliance, network security, privacy, and breach recovery.

- **eRisk Resources Directory** – From security consultants, to PCI and FACTA specialists, to forensic investigators, to e-discovery specialists, the eRisk resources directory helps you quickly find external resources with deep experience in pre- and post-breach disciplines. Information about their services, pricing, and key personnel is provided.



How Does a CFO* Rank risk?

Ranking in 2008*	Ranking in 2012*
International operations	**Information security**
Project management	International operations
Extended enterprise	Excess cash
Data privacy	Corporate culture
Fraud	Compliance
IT	**Third-party relationships**
Business continuity management	Cost reduction pressures
Shared services	Human resources
Tax management	**Social media**

*CFO.com December 2011

Questions?