MARSH

Anatomy of a Privacy and Data Breach

Understanding the Risk and Managing a Crisis

Adam Kardash: Partner, Heenan Blaikie LLP

Robert Parisi: Senior Vice President, Marsh

Leadership, Knowledge, Solutions…Worldwide.

Drivers of Privacy Risk

- Series of drivers fueling increased risks associated with privacy issues:
  - Rapid developments in information technology
  - Explosion in the volume of data
  - Transperancy of increasingly complex data flows
  - Small, yet effective privacy advocacy movement
  - Exapnding patchwork-quilt privacy legislative landscape
  - Extensive media coverate of identity theft and other fraud, security breach incidents

Drivers of Privacy Risk (continued)

- Series of drivers fueling privacy risk (con't)
  - Foreign legislative developments
  - Increased activity/profile of privacy regulatory authorities
  - Privacy recognized by privacy regulatory authorities as a governance (not a legal) issue
    - Information security governance is one part of Privacy Governance
    - New Accountability Framework

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

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

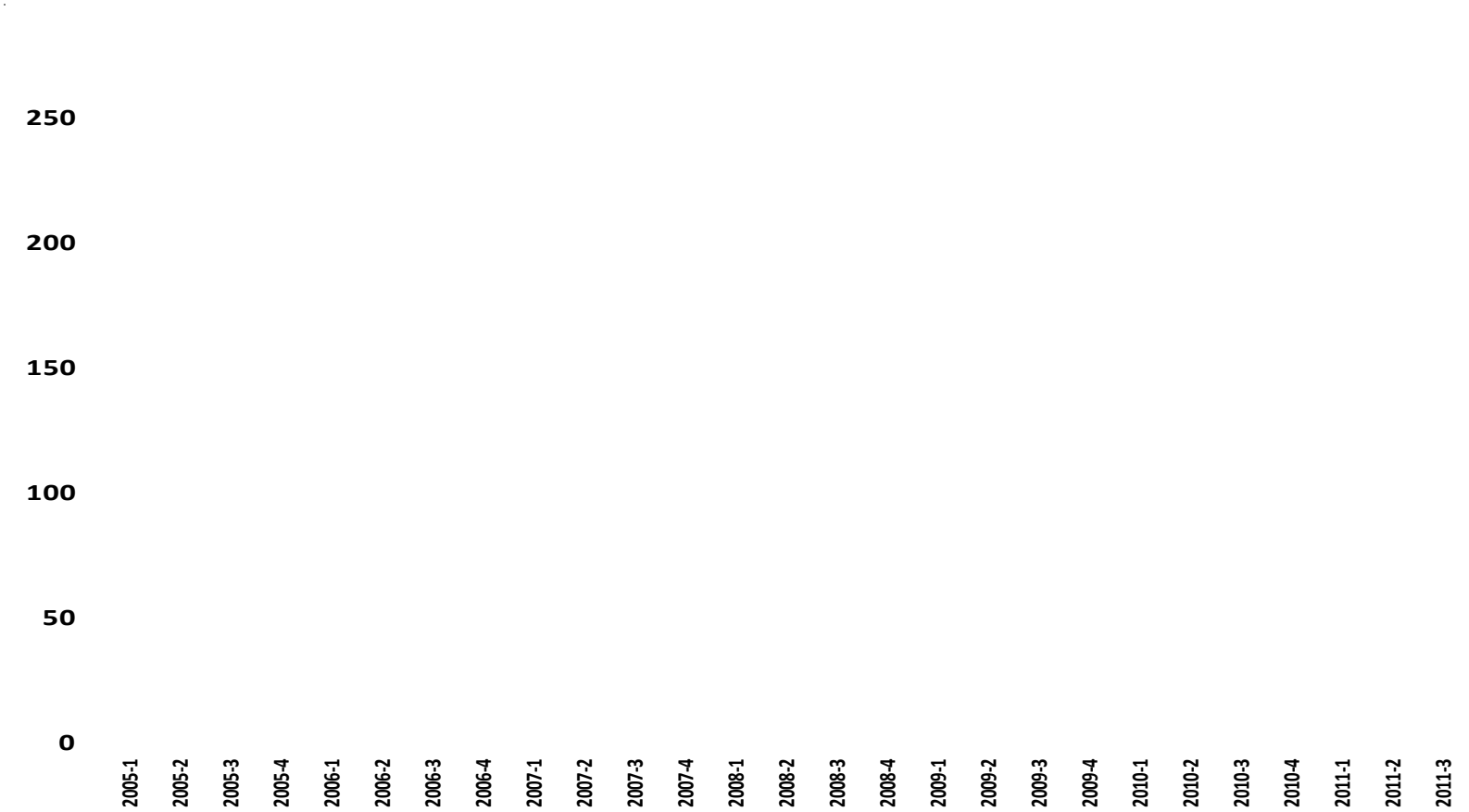
Threat Environment

- 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

Network Security / Data Risk

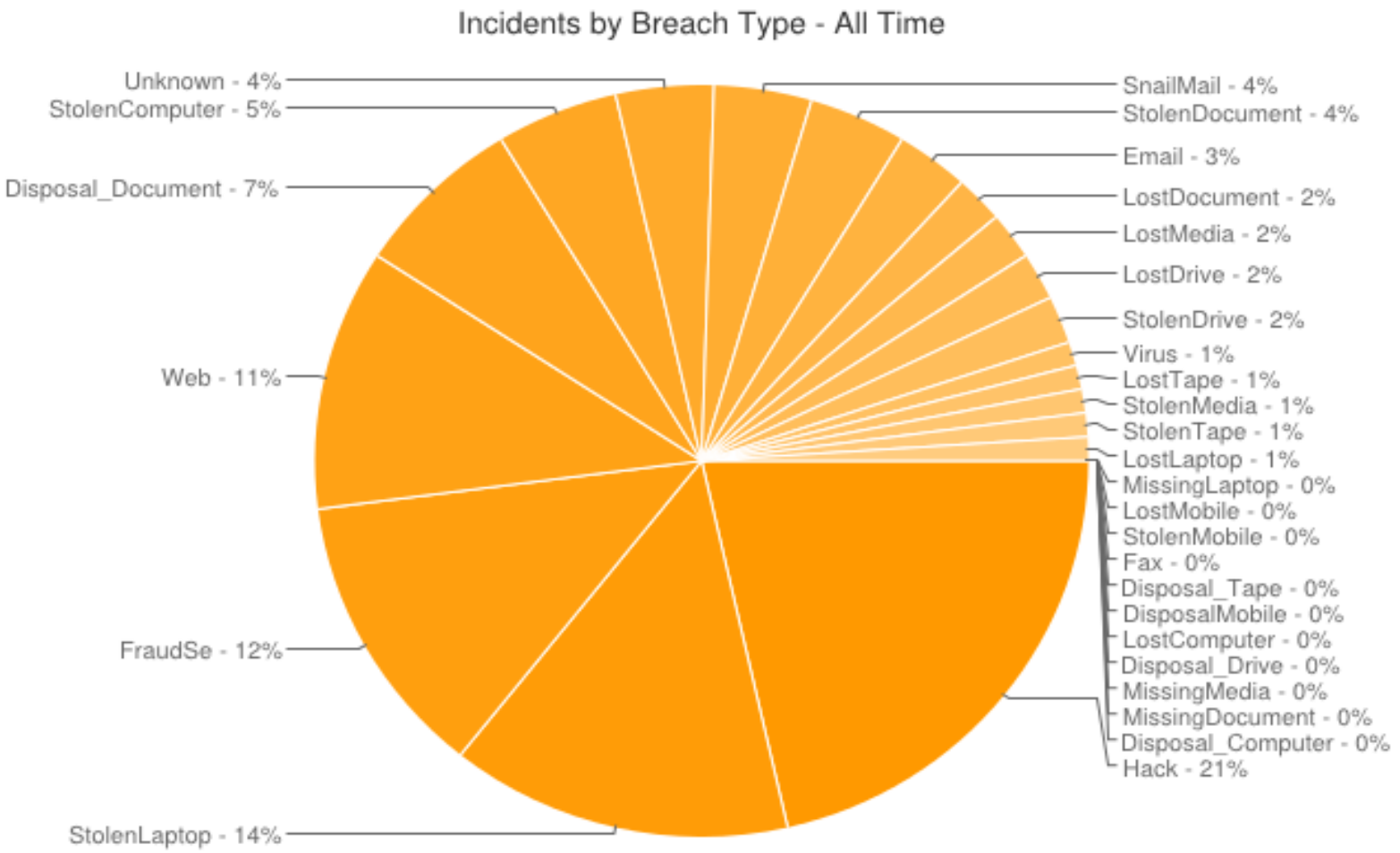
- What data do you collect?
  - Personally Identifiable Info. (PII)
  - Protected Health Info. (PHI)
  - Credit Card Numbers
- Where is it?
- How well is it protected?
- How long do you keep it?
- What is a breach?
  - Unauthorized disclosure
  - Unauthorized acquisition
  - Data compromised

Number of Data Breach Events by Year

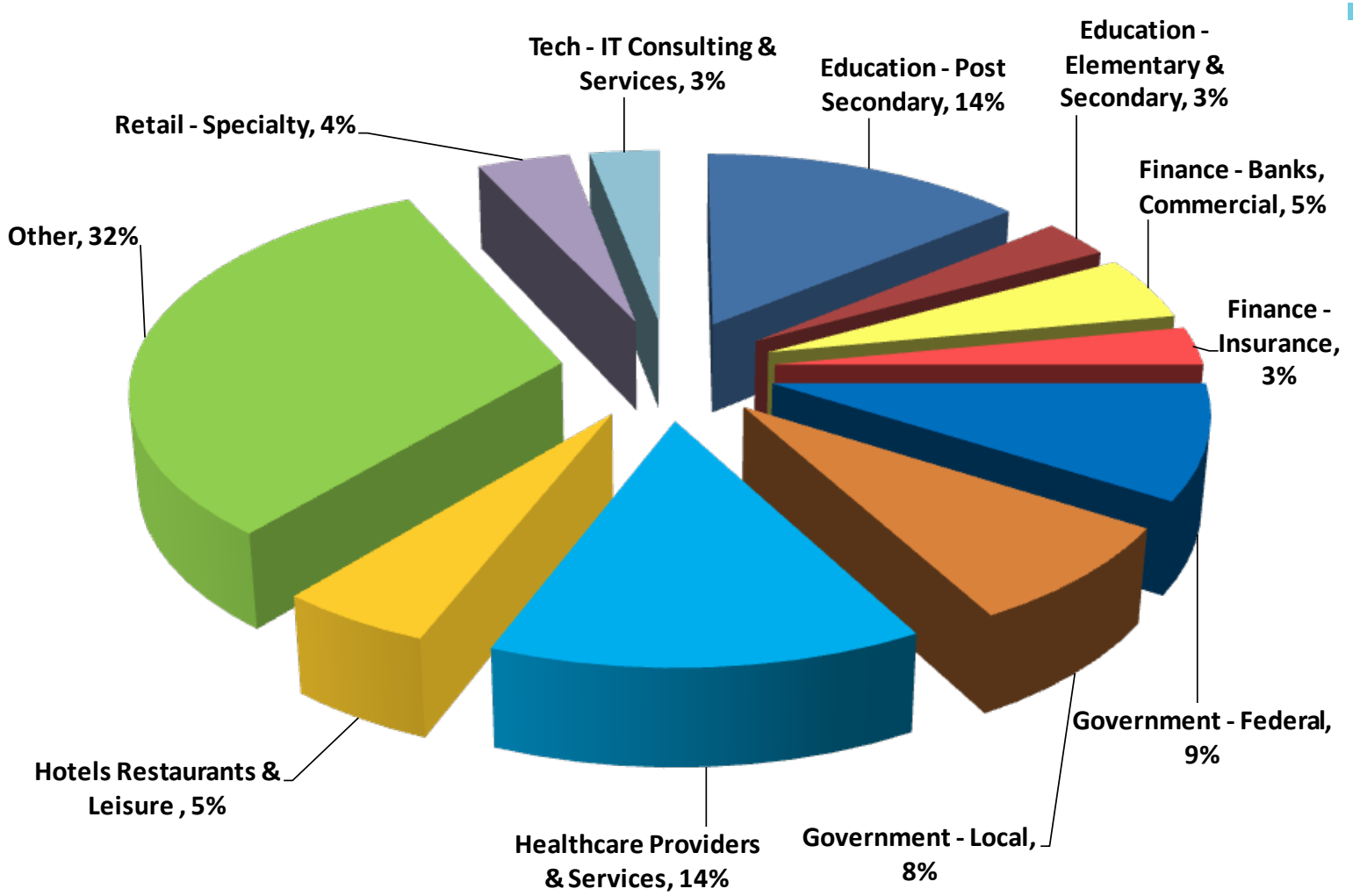


Source: Advisen MSCAd.
Includes System security breaches, other lost and stolen data, phishing, etc.

Breach Types



Percentage of Data Breach Events by Industry Segment



Sourc
Includes System security breaches, other lost and stolen data, phishing, etc.

Probable Exposure After a Breach per Data Type by Risk

	Insurable Risks				Uninsurable Risks	
	Notification Expense	Contractual Liability	Civil Liability	Regulatory Intervention	Reputational Damage	Business Disruption
SSN	**High**	**High**	Medium	**High**	**High**	**High**
Email Address	Low	Medium	Low	Low	Medium	Low
Physical Address	Medium	Medium	Low	Medium	Medium	Low
Credit Card Numbers	Medium	**High**	Medium	**High**	Medium	High
Protected Healthcare Information (PHI)	**High**	**High**	Medium	**High**	**High**	**High**
Financial Information	Medium	Medium	Medium	**High**	**High**	**High**
Drivers License or Equivalent	**High**	Medium	Medium	**High**	**High**	Medium
Customer Transaction Information	Low	Medium	Medium	Low	Medium	Medium
Other	?	?	?	?	?	?

Question – What are the implications of security breach notification requirements?

- Statutory safeguarding requirements, including notification rules, have cost and other implications for business:
  - Enhanced transperancy/reporting about security incidents within organizations
  - More notifications to affected individuals about security incidents
  - More media reports and general awareness about information security (or lack thereof)
  - More investigations by privacy regulatory authorities
  - Increased litigation risk
    - Right of “Seclusion upon Intrusion” – common law privacy tort
  - More proactive efforts by organization to address personal information security concerns
  - Increased costs to organizations to all of the above
  - Maturity of privacy risk governance

Question 1

When a major security incident involving a high volume of sensitive personal information occurs, legal counsel has a central role to play in coordinating the response to regulatory authorities and opposing counsel. From a lawyer's perspective, what are some of the hard lessons learned through the course of responding to high profile security breaches?

Lessons Learned

- Significance of effective security incident response plan cannot be overstated
- Responding to an incident is a communications management exercise

Anatomy of a Breach Event

Breach Response

1. **Fact Finding**
   - What systems were accessed/compromised?
   - What kind of data was copied/stolen? (PII, PHI, Credit Card #'s, …?)
   - How many individuals potentially affected (forensics)?
     - Where are they located?
   - Who had authorized computer access?
   - What is company security policy?
   - Who else may be involved?
     - Employees (ex-, family), vendors, acquired companies (subsidiaries, parent companies)

Anatomy of a Breach Event

Breach Response

2. Legal

- Litigation hold; notice to staff
- Develop history of system access (logs)
- Analysis of system security/ company procedures and practices/red flag provisions
- Breach Manager/coach
  - Legal compliance
  - Contract analysis
  - Notification and communication monitoring
- Litigation prep (individual, government, banks, class)

Anatomy of a Breach Event

- Breach Response
  3. Notification and Public Relations
     - Privacy Commissioner, attorney generals, credit reporting agencies
     - Affected individuals
     - Secretary of Health and Human Services (if HIPAA invoked)
     - Press conferences, news media, web and other notifications
     - Safe harbor provisions: Encrypted? Likelihood of ID theft? Alternate notice?

  4. Breach Vendors
     - Printing, mailing, and call-center services
     - Forensic IT investigators
     - Credit monitoring and/or identity theft restoration services
     - Legal counsel capable of handling potential class action/multi-district litigation in the data breach context

What Can Be Done?

Proactive Risk Manager Steps

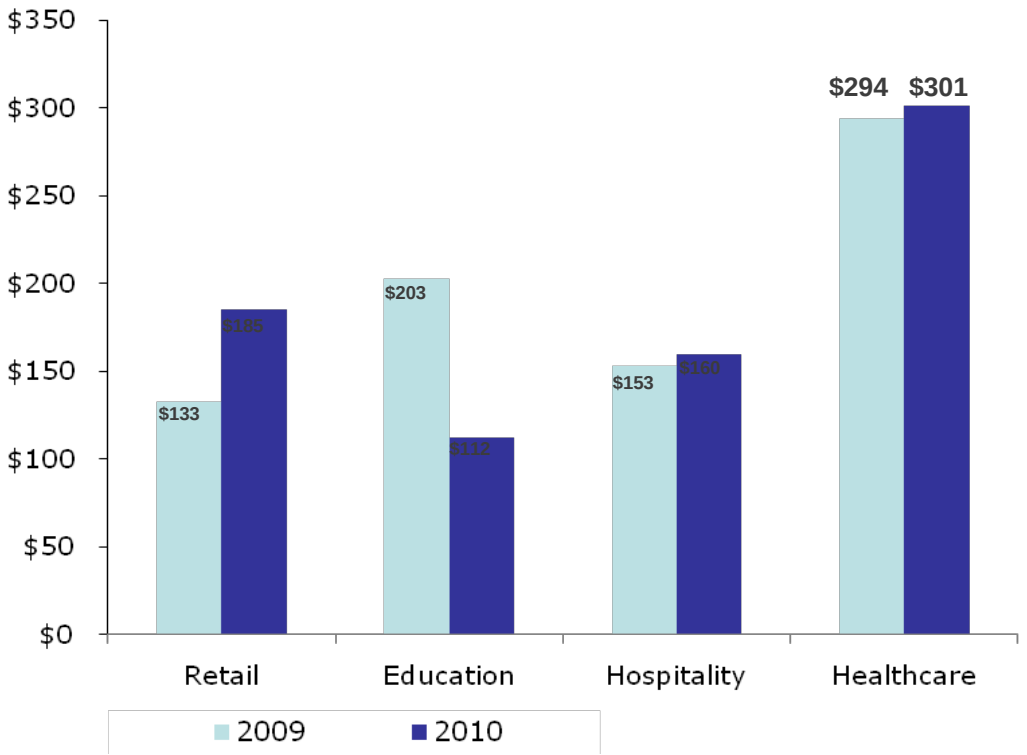
- Build an empowered senior executive
- Talk to IT security. Gain an appreciation of the many challenges.
- Can you MAP your data? Not many companies can. How many records? What type of data? Where does all this data reside? How long is it kept?
- Assess and test your own staff and operations
- Try to understand both your strengths and weaknesses
- Document your due care measures.
- Insurance
- Red flag and response plans

Easier said than done…

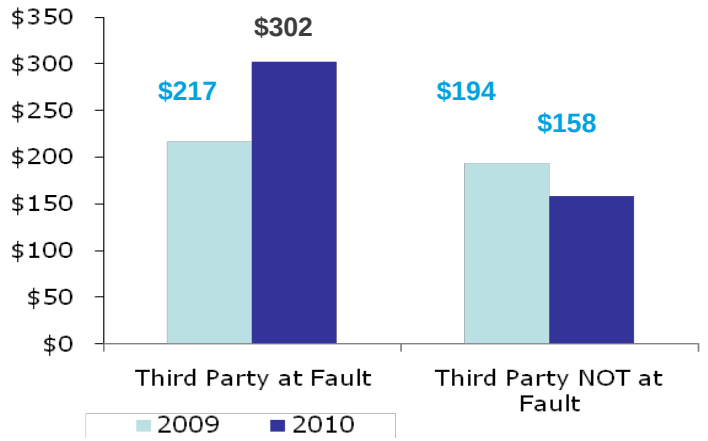
Post Breach:
Investigation and Documentation

- Has the breach been contained?
  - Isolate the affected system to prevent further exposure
- Have you engaged expert outside counsel?
  - Data forensics
  - Legal counsel
  - Breach crisis management services
  - Reputational risk advisory
- Have you considered using a third-party forensics team?
  - Credible third party assessment
  - Reliable chain of custody
  - Backups of all pertinent system logs
  - Attorney-client privilege

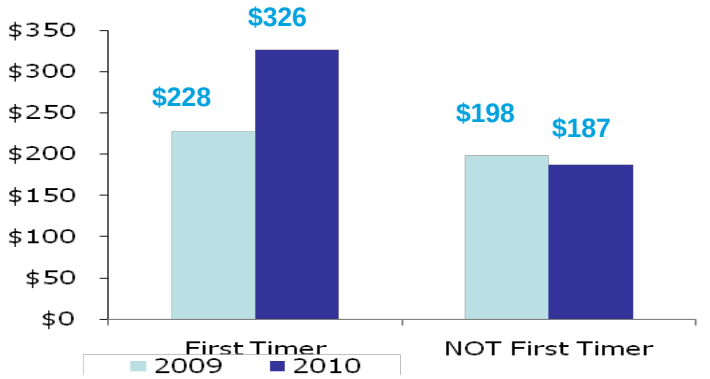
Cost per record – By Industry



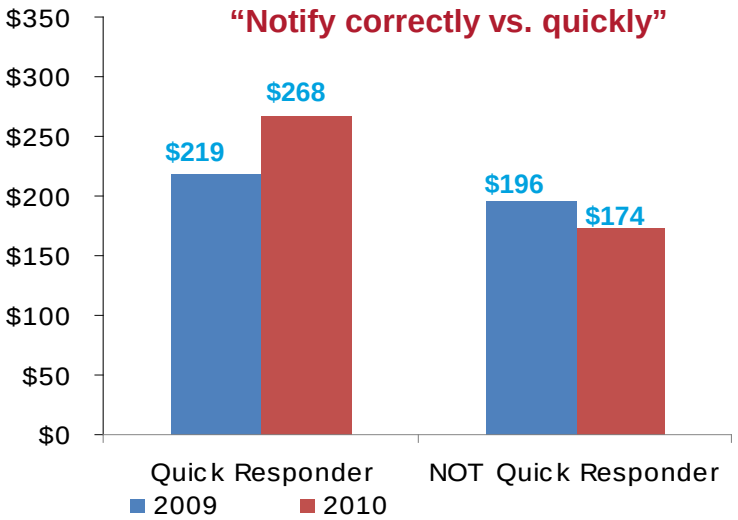
Cost per record – 3rd party related



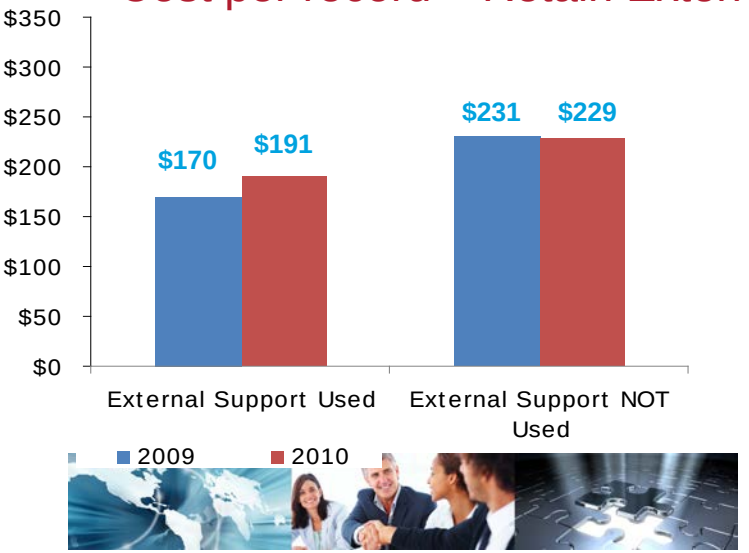
Cost per record – "1st Timers"



Cost per record – Quick Response



Cost per record – Retain External Support



CYBER RISK
CYBER RISK MODELING

Potential value of a privacy event based upon number of records compromised

Number of records compromised	100,000	250,000	500,000	1,000,000
Privacy notification costs	$400,000	$1,000,000	$2,000,000	$4,000,000
Call center costs	$100,000	$250,000	$500,000	$1,000,000
Credit monitoring cost	$1,000,000	$2,500,000	$5,000,000	$10,000,000
Identity theft repair	$500,000	$1,250,000	$2,500,000	$5,000,000
Total estimated first party costs**	**$2,000,000**	**$5,000,000**	**$10,000,000**	**$20,000,000**
Consumer Redress and Fines	$600,000	$1,500,000	$3,000,000	$6,000,000
Liability & Defense Expenses	$5,000,000	$12,500,000	$25,000,000	$50,000,000
Total estimated third party liability	**$5,600,000**	**$14,000,000**	**$28,000,000**	**$56,000,000**
Total estimated privacy event	**$7,600,000**	**$19,000,000**	**$38,000,000**	**$76,000,000**

** **Regulatory Actions:** Since a regulatory action usually proceeds the civil action, substantial expense-legal and forensic can be incurred even for events where no one is actually harmed or even at risk of harm

Assumptions:

Notification costs – $4 per record
Call center costs - $5 per call (20 percent expected participation)
Credit monitoring - $50 per record (20 percent expected participation)
Identity theft repair - $500 per record (5 percent of those monitored experience theft)

Question 2

Privacy Statues require personal information to be protected by security safeguards that are appropriate to the sensitivity of the information. These security standards require organizations to implement “reasonable” safeguard measures. From a privacy regulatory perspective, what does it mean to have “reasonable security safeguard” in today’s marketplace. What does this mean for the technology executive?

What is a “reasonable” safeguard?

- “The reasonableness of security measures and their implementation is measured by whether they are objectively diligent and prudent in all of the circumstances. To acknowledge the obvious, “reasonable” does not mean perfect. Depending on the situation, however, what is “reasonable” may signify a very high level of rigour.”

  (See BC Investigation Report F06-01)

- Findings by Privacy regulatory authorities provide the following list for organizations considering the reasonableness of their safeguards:
  - Whether the security risk was foreseeable;
  - The likelihood of damage occurring;
  - The seriousness of the harm;
  - The sensitivity of the personal information involved;
  - The cost of preventative measures; and
  - Relevant standards of practice.
    - Note: Standards set “minimum” set of expectations

  (See, for example, Alberta Investigation Reports P2006-IR-005, P2008-IR-002, and OPC and OIPC Alberta Report of an Investigation into the Security, Collection and Retention of Personal Information TJX Companies Inc. /Winners Merchant International L.P.)

Question 3

In the course of a privacy regulatory investigation in response to a security incident, what are the key questions privacy regulatory authorities want to know from the organization?

Be prepared to respond to the following four questions during a privacy regulatory investigation of a security incident:

1. Show us your organization's security incident protocol, and how you implemented it?
2. Show us your organization's information security governance program?
3. Show us evidence of your regular compliance monitoring.
4. Show us evidence of regular training and awareness.

Thank You

MARSH

Robert Parisi
Senior Vice President, FINPRO
National Practice Leader for Tech/Telecom E&O and Network Risk

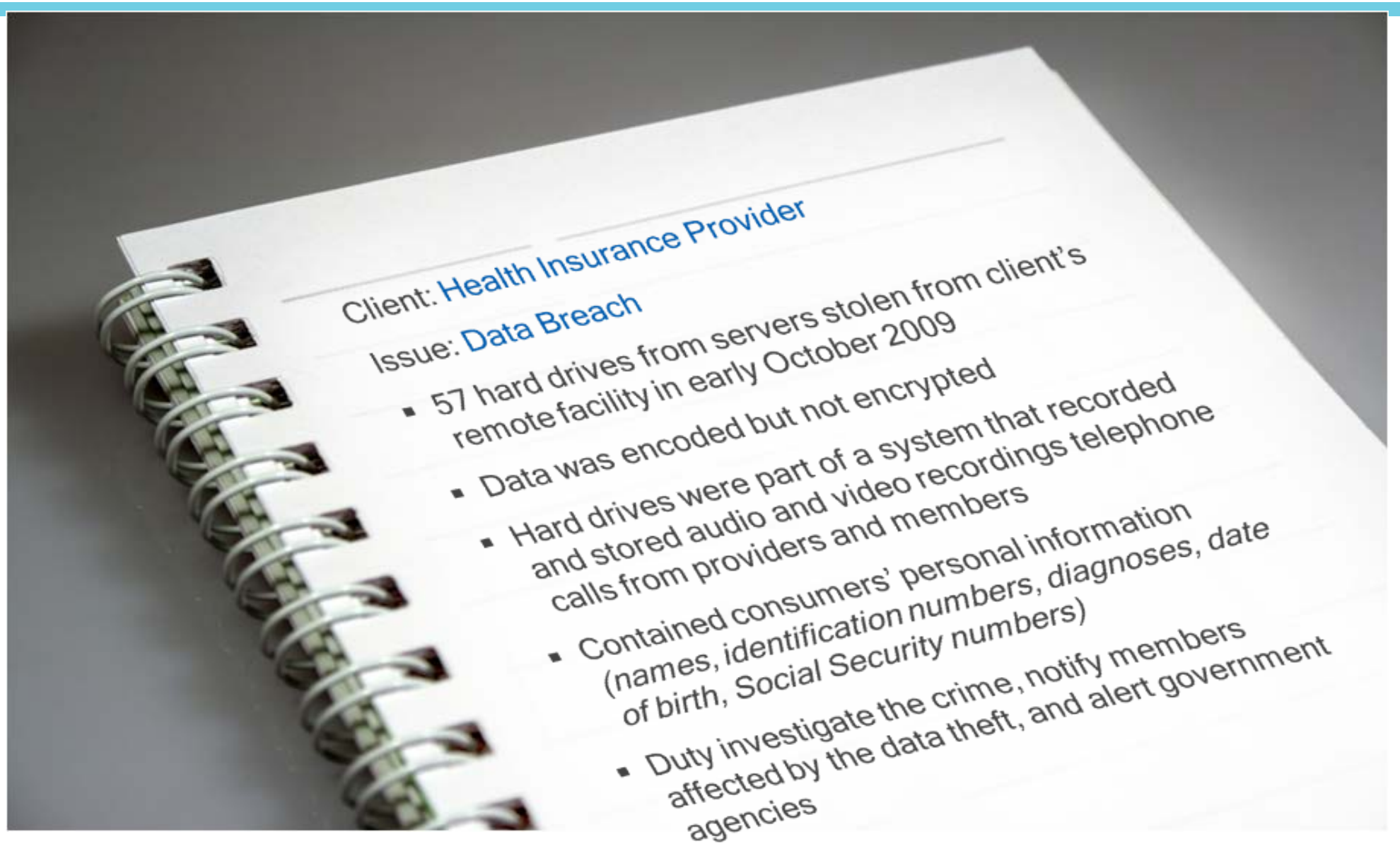
Marsh
1166 Avenue of the Americas
New York, NY 10036

Office: 212.345.5924

Email: robert.parisi@marsh.com

For More Information: www.marsh.com

Case Study #1
Situation



Case Study #1

Use of third party forensics experts is often critical to the investigation and breach remediation and notification process.

- Information Security/Breach Assessment
  - Gathered facts from numerous sources to determine scope of breach
  - Responded and located backup tapes of stolen data
  - Data review services, computer forensics, data recovery and information security consulting
  - Rebuilt server environment based on backup tapes, with assistance of data recovery and computer forensics teams
  - Exhaustive inventory of all data included on the drives; including reviewing data for consumers' personal information
  - Information security assessment and penetration test (on-going)
- Enhanced Identity Theft Consultation and Restoration Services
  - Member notifications (approximately ½ million notifications delivered)
  - Identity theft restoration

Case Study #1
Solution Continued

- **External Infrastructure**
  - One isolated network and two video servers
  - 210 computers
  - Five review rooms with tables/desks and chairs

- **Data**

  Audio
  - Received 3,167,619 audio file
  - Reviewed 1,206,239 audio files (after searching/filtering)

  Video
  - Received & reviewed 160,110 video files

- **People**
  - 420 reviewers (a total of 89,700 labor hours)

- **Timing**
  - 7.5 weeks of review
  - Approx. two weeks of initial planning and final production
  - Two shifts, Monday – Saturday (6:30am – 4:30am)

Best Practices
Breach Preparedness and Prevention

- Maintain a cyber risk transfer instrument
- Have a proper background screening program for new hires and vendors
- Pre-arrange a breach service provider, outside counsel, and reputational risk advisor, all specializing in privacy law and breach crisis management
- Provide “certification” through e-learning to employee base on safeguarding data
- Develop an incident response plan
  - Internal staff
  - Outside counsel
  - Reputational risk advisor
  - Breach service provider

Best Practices
Breach Preparedness and Prevention (cont.)

- Conduct annual risk assessments and tabletop exercises
- Hold an internal “privacy summit” to identify vulnerabilities
  - Risk
  - Compliance and privacy
  - HR
  - Legal
  - IT
  - C-level representation (CFO)
  - Physical security/facilities
- Keep general counsel’s office current to various state disclosure laws and updates
- Shredders – Post office boxes, cafeterias, dorm lobbies

Best Practices
Breach Crisis Management

- Retain an outside counsel who specializes in privacy law and breach crisis management
- Notify correctly vs. quickly
  - Diffuse anger and emotion among constituents
  - Provide remedy with notification
  - Identity an accurate breach universe to minimize public exposure to event
  - Unique constituents
- Leverage an outside call center
- Retain a reputational risk advisor who specializes in breach crisis mnagement
- Investigate, investigate, investigate!
  - Have outside counsel retain any data forensics investigation
  - Potentially minimize public exposure to event
- Leverage a breach service provider to conduct recovery
  - Pre-existing ID theft victims
  - More thorough recovery and restoration