

# Surviving a Data Breach

25<sup>th</sup> Annual Windy City Summit  
May 19, 2011  
Peter Foster

The Willis logo consists of the word "Willis" in a white, serif font, centered within a dark blue rectangular box. This box is positioned on the right side of a horizontal yellow bar that spans the width of the slide.

**Notes:**

---

# Network Security / Data Risk

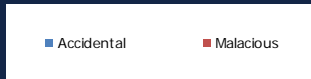
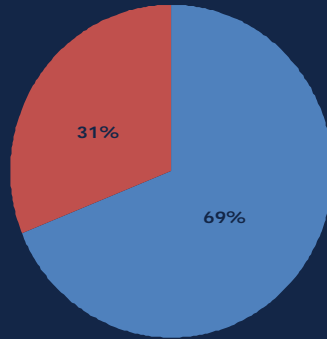
- What do you collect
  - Personally Identifiable Information (PII)
  - Protected Health Information (PHI)
  - Credit Card Numbers
- Where is it?
- How well is it protected?
- How long do you keep it?
- What is a breach?
  - Unauthorized disclosure
  - Unauthorized acquisition
  - Data compromised

Willis

**Notes:**

---

# Malicious v. Accidental – 2010 Frequency



© Ponemon Institute 2011

Willis

**Notes:**

---

# Lawsuits come from...

- Single Plaintiff
  - Identity theft
  - Privacy
- Government (Regulatory) Action
  - Attorneys General
  - FTC Commissioner
  - Secretary of Health & Human Services (HIPAA)
- Banks
  - Cost of replacing credit cards
  - Reimbursement of fraudulent charges
  - Business Interruption
  - Industry standards violations
  - Reimbursement of legal fees

Willis

**Notes:**

---

# Key US Regulations

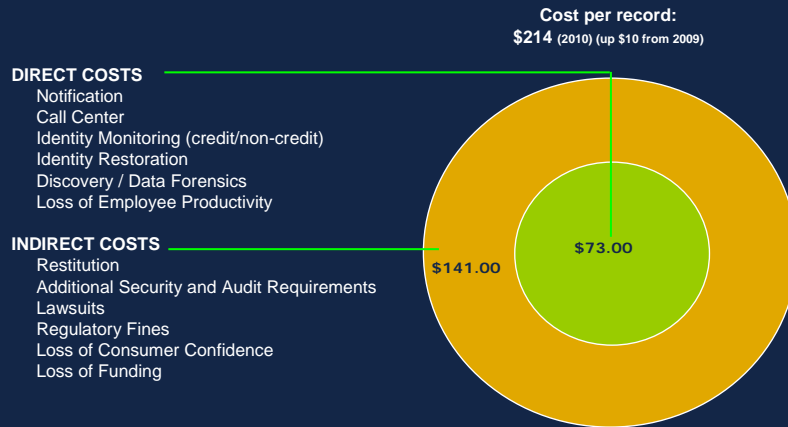
- HITECH
  - National Breach Notification Requirement; Extends HIPAA to “business associates” (BAs)
  - BAs – “independent contractors” vs. “agents” – big difference
  - Requires Identity Theft Prevention Program
- FACTA
  - Red Flags Rule: Requires Identity Theft Prevention Program
- State Notification Requirements
  - Notification required in 46 states + 3 territories
  - Massachusetts, Minnesota, and Nevada now mandate specific IT protocols and practices (encryption, compliance with PCI DSS, proactive monitoring and security programs)
- SOX, Graham Leach Bliley (GLB)

Willis

**Notes:**

---

# Cost of a data breach



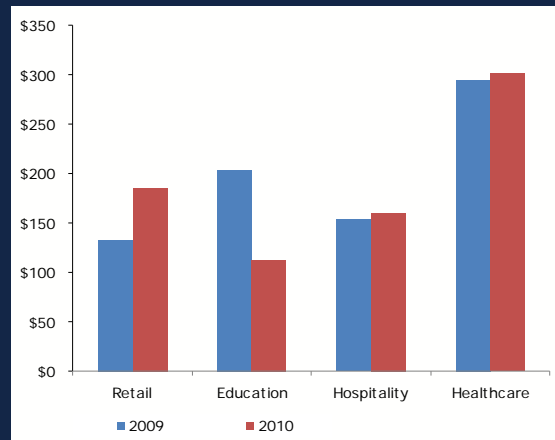
© Ponemon Institute 2011

Willis

**Notes:**

---

# Cost per Record – By Industry



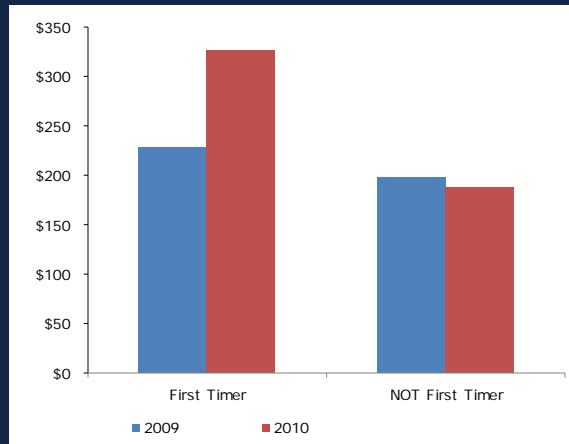
© Ponemon Institute 2011

Willis

**Notes:**

---

# Cost per Record – "1st Timers"



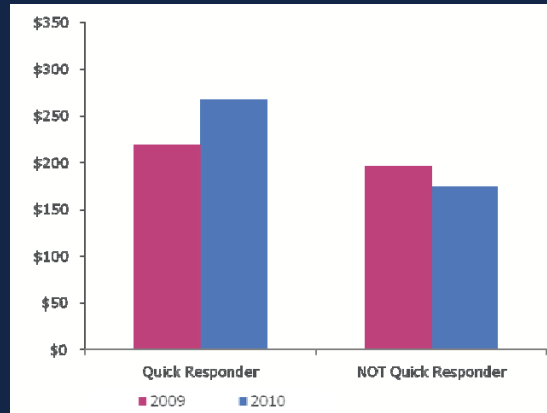
© Ponemon Institute 2011

Willis

**Notes:**

---

# Cost per Record – Quick Response



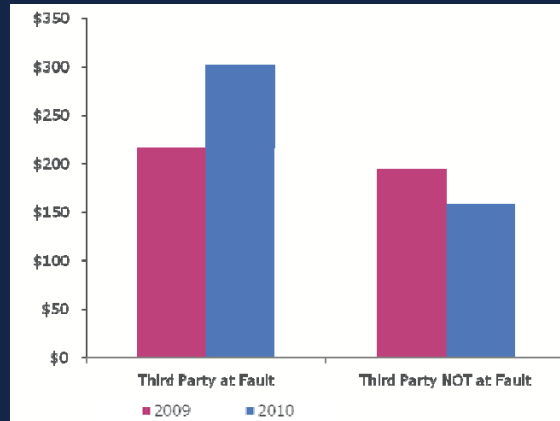
© Ponemon Institute 2011

Willis

**Notes:**

---

# Cost per Record – 3rd Party Related



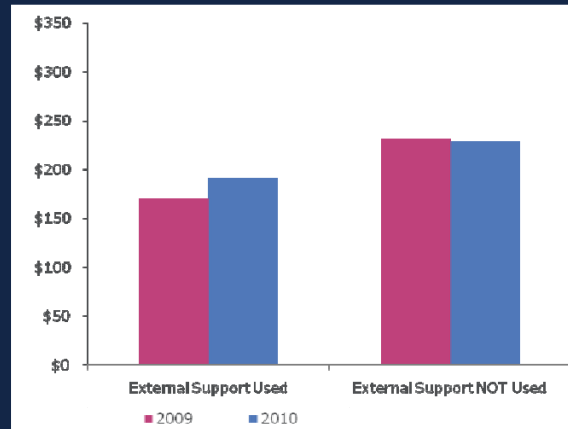
© Ponemon Institute 2011

Willis

**Notes:**

---

# Cost per Record – Retain External Support



© Ponemon Institute 2011

Willis

**Notes:**

---

# Prepare / Prevent

## Steps

## Challenges

## Response

Identify

- What information exists?
- Where is it?
- What format is it in?
- How easy or difficult is it to access?
- Are the systems and networks that hold the data secure?

- Data Mapping & Inventory
- Table Top Exercises
- Data Accessibility Assessment
- Data Security Assessment and Strategy
- Vulnerability Testing
- Credit Monitoring
- Network Monitoring

Comply

- Do you know what your regulatory and compliance requirements are? Are you meeting them?
- Are you familiar with international data privacy laws that impact your business?
- Do you have a records retention schedule and policy?
- Are you utilizing storage technologies that will support your compliance with regulatory requirements?

- Records Retention Consulting
- Data Preservation and Collection
- Compliance and Global Data Privacy
- Data Archiving
- Incident Response

Protect

- Do you have a response plan should a breach incident occur?
- Are you securely destroying data and storage that has met the end of its retention period or life cycle?

- Incident Response Strategy

Willis

**Notes:**

---

# Respond / Remediate



**Notes:**

---

# Best Practices – Breach Preparedness and Prevention

- Have a proper Background Screening Program for new hires and vendors.
- Review contracts with IT vendors, assuring they are compliant with regulatory bodies, provide appropriate indemnification and carry Privacy Liability Insurance.
- 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, based on safeguarding data
  - #1 preventative initiative being adopted by CISOs and CPOs in 2010 (as per Ponemon 2011 study)
- Keep General Counsel’s office current to state disclosure laws, federal regulations, foreign requirements and updates (Reference material – Perkins Coie State Law Update; Baker & McKenzie Global Privacy Guide).

Willis

**Notes:**

---

# Best Practices – Breach Preparedness and Prevention

- Develop an Incident Response Plan (required in many federal & state laws – HITECH, MA201, et al.)
  - Internal Staff, Outside Counsel, Reputational Risk Advisor, Breach Service Provider
- Conduct annual Risk Assessments and Tabletop Exercises – Focus on:
  - Encrypting all laptops and portable media (jump drives, tapes, etc.) enterprise wide
  - Access Controls (Employee risk in a down economy)
  - Data Classification
  - Incident Response
  - Vendor Management
- Hold an internal “Privacy” workshop to identify vulnerabilities. Attendees should include:
  - Risk Management, Compliance and Privacy, HR, Legal, IT, C-level representation (CFO), Physical Security/Facilities, Procurement (IT Vendor Relationships), and Internal Audit
- Consider Privacy and Network Security (Cyber Risk) Insurance as a financial protection

Willis

**Notes:**

---

# Best Practices – Breach Crisis Management

- “Notify Correctly v. Quickly”
  - Decision-tree process internally – Who makes the final decision?
  - Diffuse anger and emotion among constituents
  - Provide remedy with notification (if necessary) – If your IT vendor breaches your customer or employee data, you must control the message in the notification
  - Identify an accurate breach universe to minimize public exposure to event
- Investigate
  - Have outside counsel retain any data forensics investigation
  - Potentially minimize public exposure to event – Compliance requirements?
- Leverage a Breach Service Provider to conduct Recovery
  - Pre-Existing ID Theft Victims
  - More thorough recovery and restoration – reduce overall liability exposure
- Notify your Privacy & Network Security Insurance broker and insurer as soon as practicable

Willis

**Notes:**

---

# Privacy & Network Security Insurance

## Consider the following:

- Privacy Liability – Coverage from the breach of Personal Identifiable or Health Information (i.e. Employee Benefits) or Corporate Confidential Information, including class action suites – whether done intentionally or negligently; internal or external, including by a vendor
  - Regulatory Defense Expenses and Fines/Penalties/Consumer Redress following a data breach;
  - Privacy Expenses (Mandated or Voluntary Notification costs, credit monitoring, PR/Crisis Expenses, Legal Compliance costs);
  - Network/Privacy breach Forensic expenses
- Network Security Liability – Coverage for 3rd party financial losses due to the compromise of your security (i.e. hacker disruption if a client-facing application causes your client loss off income; DDOS attack causes a loss 3rd parties)
- Multimedia Liability – Coverage for publishing and advertising liability not covered under your General Liability policy
- 1st Party Data Damage/Business Interruption – Costs due to hacker/virus/employee sabotage/cyber terrorism/administrative error
- Cyber Extortion

Willis

**Notes:**

---

Questions ?

Willis

**Notes:**

---

Peter Foster

(p) 617-351-7480

(e) peter.foster@willis.com

Willis

**Notes:**

---