



# Challenges to deal with Data Breach

**Muzaffar I. Chaudhary CISA, CISSP**

**08/30/10**



# Agenda

- I. Background
- II. GA Data Breach Law
- III. Regulatory Requirements
- IV. A Data Breach Scenario
- V. Incident Management
- VI. Pro-active Approach to Incident Management
- VII. 5 Steps to Manage a Data Breach
- VIII. Q&A



# Major Headlines In the news

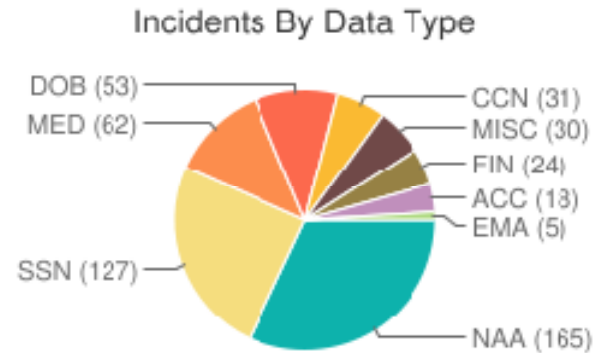
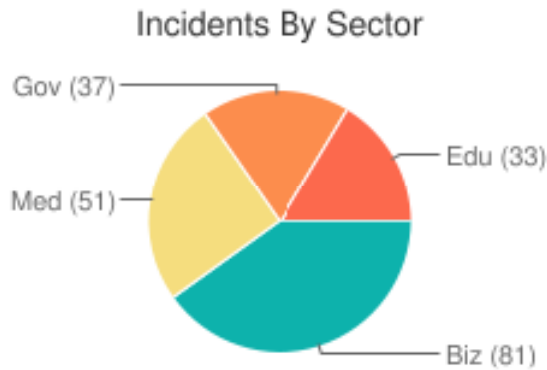
- **15 years jail time for TJMax Hacker- Sept. 2009**
  - 45.7 million credit and debit card numbers stolen
- **Second Breach in Data at Berkeley University - August 2009**
  - Breach of Social Security # and Birth date of 493 students



# Data Loss Database - 2010 yearly report

Total Incidents: 199

Total Records Affected: 13,680,910



Source: [datalossdb.org](http://datalossdb.org)



# The Data Breach Landscape

- **50% More data breaches in 2009 than in 2008 with and estimated 35.7m individuals affected (Washington Post)**
- **32%: Percentage of respondents who say that security breaches in the past year resulted in alterations to software applications**
- **80%: Number of respondents that stated their organization does not have mechanisms in place to report incidents to customers or authorities**
- The “insider threat” appears to be on the rise. In 2008, the percentage of respondents who cite **employees as the likely source of attack increased significantly (51% vs. 30%)**
- **69%: Respondents that do not keep an accurate inventory of where data is stored**
- **21%: Percentage of CISO/CSO’s that state their organization is not compliant with state privacy breach laws**



# Data Breach Readiness



When it comes to a data breach, the question is not “if” you will become a target, the question is “when.” Operational preplanning and readiness can control costs, improve customer loyalty and preserve your reputation.



# Georgia Breach Law

The law requires that "Any information broker that maintains computerized data that includes personal information of individuals shall give **notice of any breach** of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."



# Regulatory Requirements (PCI, HIPAA..)

1. **Isolate the breach-** for Forensics
2. Inform **necessary parties** – Law enforcement etc.
3. **Notify** your business partners (e.g. Bank)
4. **Incident Response Report**



# PCI Requirements

## Develop Incident Response Plan

### Requirement 12.9:

12.9.1: **Create an incident response plan**

12.9.2: **Test the plan at least annually**

12.9.3: **Designate specific personnel to be available on a 24/7 basis to respond to incidents**

12.9.4: **Provide appropriate training to staff with security breach response responsibilities**

12.9.5: **Include alerts from IDS, IPS and file integrity monitoring systems**

12.9.6: **Develop processes to modify and evolve the IR plan according to lessons learned**



# A Data Breach Scenario (hypothetical)

Credit card data is compromised at the Airport. The DOA has to notify the effected customers according to “GA Breach Law Notification”. The Executive Management at DOA has asked the Public Relations, Information Security Officer and DOA’s Attorney to do the following:

- A press release to the media for the incident
- A posting on DOA Website for the incident
- Letter to the effected customers whose credit card information have been stolen



# A Perfect Storm



This breach event may become ultimate nightmare, a “perfect storm” if:

- DOA Customers learned of the breach via sensationalized **media reports**.
- DOA was obliged to make public statements in the **absence** of necessary facts.
- Card Issuers had to act quickly, with **little** information, to notify customers and determine if cards should be closed and new cards reissued.



# Pro-active Approach to Incident Management

- **Data Steering Committee (Event Response Team )** consisting of key executives and personnel from areas of the business that would be affected by a data breach.
- **A Risk Assessment and Response Matrix** that guides your team in determining how harmful a particular breach event would be and how you should respond to it.
- **A Communication Plan** designed to control outbound messaging related to the event and to maintain public confidence

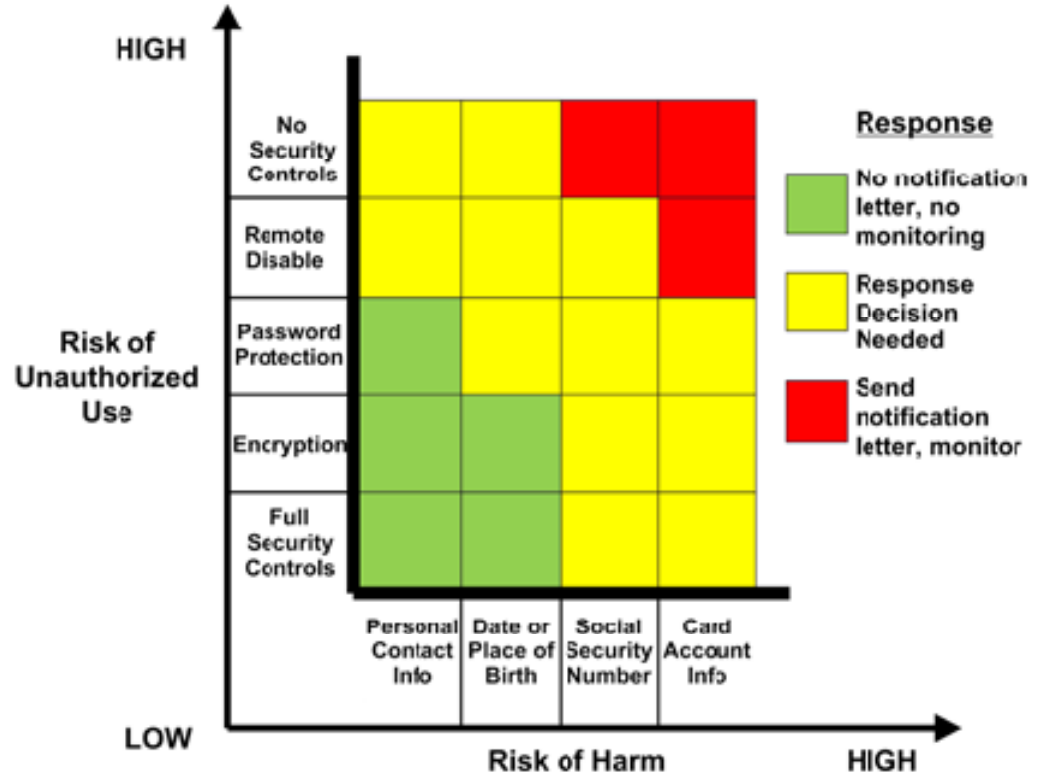
# Building Your Data Steering Committee



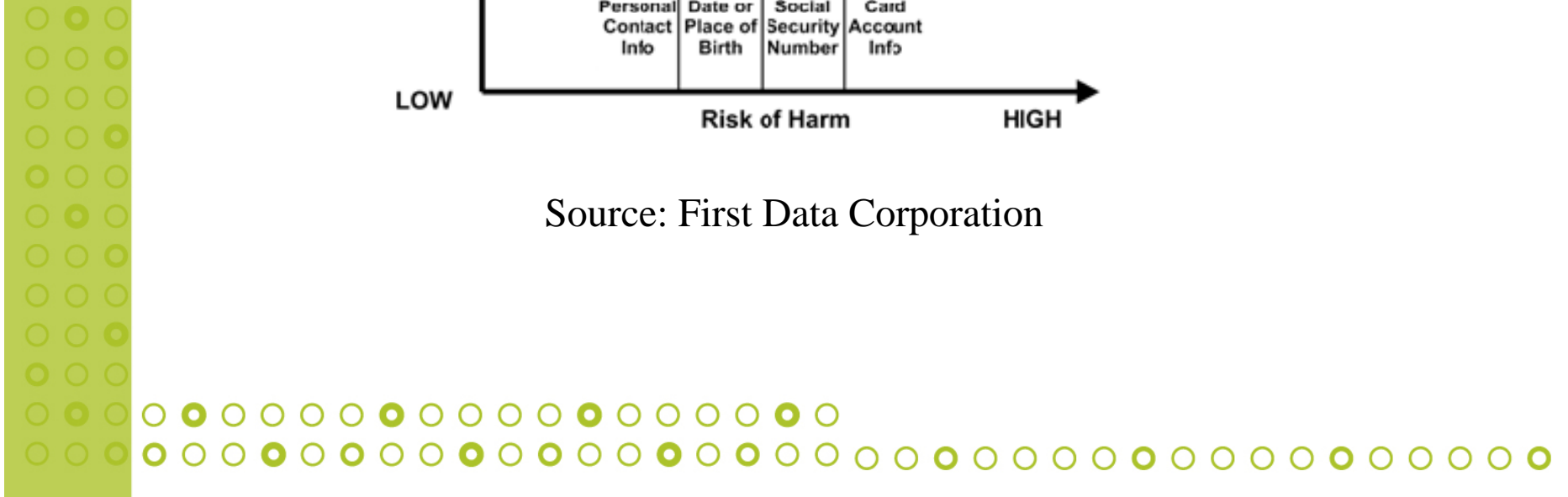
- Audit and compliance
- Representatives from all customer-facing groups
- Human resources
- Key executives and senior decision-makers
- Legal
- Marketing and public relations
- Operations/information technology
- Risk management and Information security



# Creating Your Risk Assessment and Response Matrix



Source: First Data Corporation



# A Solid Communication Plan



- When a breach is contained, announce what you know when you know it.
- If there are things you do not yet know—perpetrator, details of attack etc. Avoid spreading misinformation that you will eventually have to correct or retract.
- Explain why you cannot reveal certain information.
- Describe, in specific detail if possible, what you are doing and why you are doing it.
- Be honest, above all else. Your customers and partners will appreciate it.



# Bad-News Management Plan

- Prepare for the worst by envisioning the best
- Go from start to finish in words and pictures
- Do a dry run
- Establish leadership contingencies
- Coach and train spokespeople



# Five Steps to Manage a Data Breach

1. Define process to **Investigate a Data Breach**
2. Process to Deploy **Incident Response Team**
3. Create / Implement **Notification Plan/ Communication Plan**
4. Perform a **Response Audit** after the event
5. Conduct **tabletop exercise** at least once a year



# Any Questions ?

Q and A



# Supporting Slide Security Risk Assessments

- External ASV scan of all active hosts **quarterly**
- **Annual** network penetration test (internal & external)
- **Annual** web application test on all externally exposed web apps.
- **Annual** risk assessment
- Regular internal vulnerability assessments

