

S31 - Incident Response Clinic

Kieran Norton



September 21, 2009 – September 23, 2009

Incident Response Clinic

Kieran Norton, Senior Manager,
Deloitte & Touche LLP



September 21, 2009 – September 23, 2009



Current Landscape

What

Large scale breaches and losses involving credit card data and PII (SSN, etc.)

- Heartland
- RBS Worldpay
- Hannaford
- TJX
- Veterans Affairs
- HM Revenue & Customs
- Etc.*

Customer data sold by "trusted" parties

- Countrywide Financial
- Sprint

Accidental disclosures

- Occur almost weekly*
- Exposure, loss, transport, etc.

How

Organized crime

- Global, employs multiple approaches (see below)

Hacks

- SQL injection, trojans, sniffers, custom malware, 'drive by' attacks, etc.

Insiders

- Typically leveraging existing privileges

Theft

- Stolen laptops, computers, etc.

Losses

- Backup tapes, thumb drives and other media

Human or IT system errors

- Resulting in disclosure of sensitive information

*Fun Reading:

<http://www.privacyrights.org/ar/ChronDataBreaches.htm#Total>

<http://www.databreaches.net/>

http://datalossdb.org/search?direction=desc&order=reported_date&page=1&query=



Drivers for Incident Response

Unauthorized access laws

- Force emphasis on types of sensitive information – but not just about financial data anymore
- Notice
- Encryption
- State may take action

Reasonable security program standards/rules

- Forces focus on holistic approach
- Calls for incident response (IR) program
- Program must be documented, risk based, part of infosec program
- The yard stick by which one will be measured if there is a breach

Federal Action / Consent decrees

- “Do what you say you do”
- Oversight
- Known vulnerabilities

Private Actions

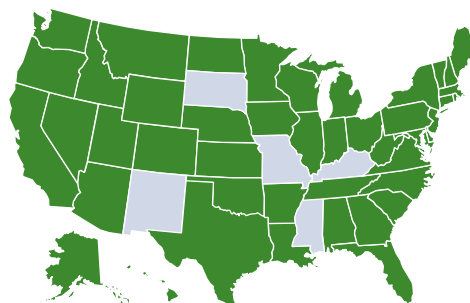
- Liability (state’s laws)
- Contractual obligations and penalties (PCI)



Requirements Outpace Organizations

Business organizations have been significantly impacted by the increase in regulatory and industry requirements (such as PCI) to report breaches of personally identifiable information (PII) to data subjects or business partners.

Driven by breach notification laws in nearly all states, breach notification requirements expose businesses to potentially significant losses arising from negative publicity, loss of reputation, regulatory fines and class action lawsuits.



□ No legislation enacted ■ Legislation enacted

Traditional security measures are proving inadequate to prevent unauthorized access to data (external and internal, intentional and unintentional), and attacks are increasingly sophisticated and far reaching.



Common Challenges

In assisting clients dealing with breaches, a few common challenges have been noted:

- Misunderstanding of risks, misplaced trust
- Limited understanding of where sensitive data is collected, used, stored, shared and destroyed
- Insufficient emphasis on secure coding practices and security QA
- Permissive access
- No information classification
- Flat architecture
- Duties not segregated
- Third-party connectivity/access
- No Asset Controls, Limited Physical Controls
- End-user computing vulnerabilities
- Limited role and activity-based training/guidance
- Limited incident response capability

Where the trouble starts:

Disconnect between corporate privacy and security policies, actual operational practices and technology infrastructure



Are All Breaches Created Equal?

Incidents can take many forms, not all will involve customer data or notification requirements, but all must be dealt with and the line between them is continuing to blur:

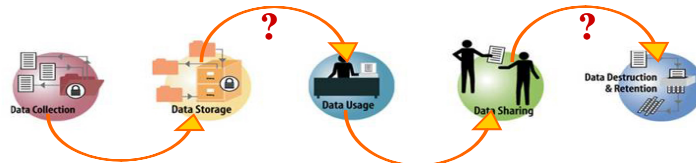
- Unauthorized access
- Malicious code / software
- Denial of Service
- Inappropriate usage (and behavior)
- Attempted access (probing, scanning, attacks, etc.)
- Compound incidents

While many of the following discussion points will focus on breaches affecting consumers and related responses, the material applies to all of the above types and a strong incident response program will deal with multiple incident types



Incident Response Program

- A company's IR program should be part of its overall information security and privacy program(s)
- Building an effective IR program requires businesses to better understand the threat and the target
- Organizations can proactively reduce the likelihood of a data breach by identifying data assets and evaluating business process risk throughout the data life cycle



- The program should be framework based and response should be:
 - Thought through (considered, intentional, appropriate, complete)
 - Risk-based
 - Tactical *and* strategic



Incident Response Program (Cont')

- Early issue spotting is critical:
 - Lost data may have the same consequences as a hacking incident
 - Notice (who to tell, what to tell and when) may not be simple
 - Duties and obligations may not be clear and might conflict (customers, partners, regulatory agencies, law enforcement)
- Post-incident analysis is essential
 - Address the root-cause
 - Understand what went well, where there is room for improvement
 - Update the program based on lessons learned
- Practice does not make perfect...but it does make better
- Dusting off an old IT focused IR program will not work given the complexities discussed in the prior slides



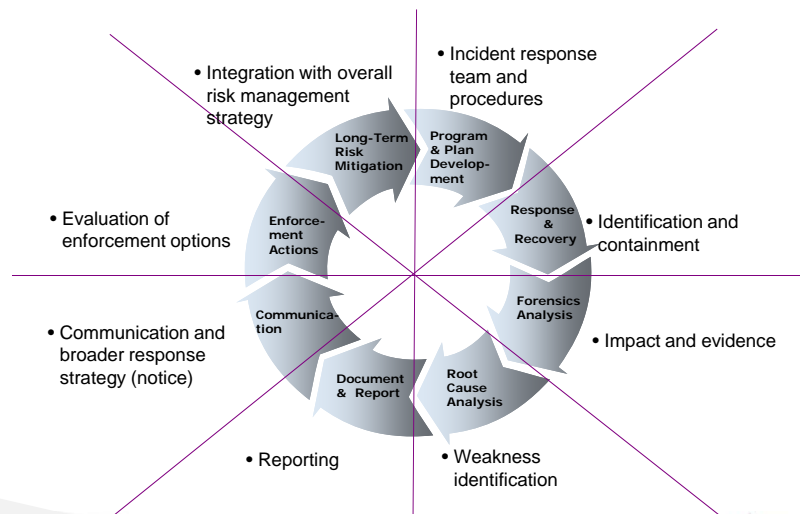
Incident Response Framework

Objectives of incident response framework:

- Confirms or dispels whether an incident occurred (and to what extent)
- Promotes accumulation of accurate information for action by responders and management
- Establishes controls for proper retrieval and handling of evidence
- Protects privacy rights
- Minimizes disruptions to operations
- Allows for legal or civil action against perpetrators
- Provides accurate reports and recommendations for improvement



Incident Response Process Overview



Responding: Pre-Incident Preparation

Roles should be defined

- Investigative team
- Response team
- Cross-functional participation
- Executive participation

Response strategy formulated

- Policies and procedures
- Training/practice
- Pre-canned responses
- Involve the right people at the right time

Detection mechanisms/monitoring

- Importance of logging and monitoring – where, what, how

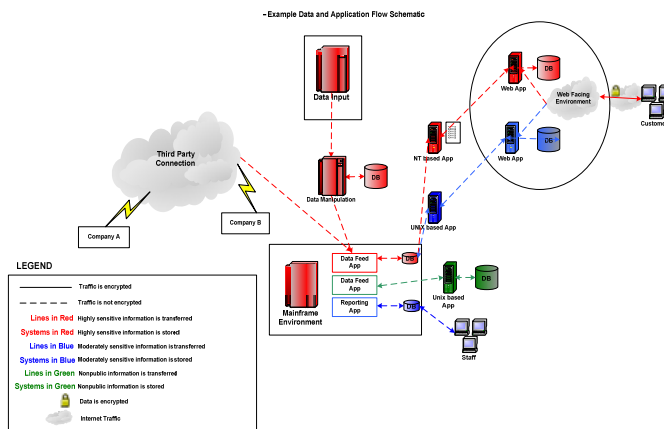
Asset controls

Patch/vulnerability management



Responding: Pre-Incident Preparation

Know where your data is!



Responding: Investigation

Investigation:

- Obtain basic facts and establish the circumstances (question what is learned)
- Preserve evidence (chain of custody, if warranted)
- Assess the nature and scope of the incident, including which customer information systems and what specific elements of customer information have been accessed or misused
- Consider a scenario-based investigation approach in circumstances where the impact is known but the source of the breach is vague

Worth Noting:

- Logging and monitoring is critical to *detecting and scoping* a breach – too often clients find that they don't have sufficient logging in place when they need it most
- Many breaches involved repositories of sensitive information that the client had not identified
- Know thyself: do you have the right skills to respond or do you need help?



Responding: Investigation (Cont')

Response Strategy:

- Perform a risk assessment to enable the company to determine the scope and risk of the incident, and how to respond to the incident
- Perform appraisal of incident's impact on company systems, data or business. Consider:
 - System downtime
 - Number of users/customers effected
 - Monetary loss incurred
 - Reputation loss incurred
 - Client losses (financial, reputation, etc.)
- Determine which, if any, regulatory and/or law enforcement agencies require notification, and whether there are additional notifications

Worth Noting:

- You should involve your legal team, but be aware if you are taking action based on a literal or narrow interpretation of the facts and relevant law



Responding: A Note on Notification

Are notifications required?

- Are there regulatory obligations that require notification?
- Are there contractual obligations that require notification?
- Are there other external parties that the company would choose to notify?

Potential individuals/entities to notify include:

- Individuals/data subjects affected
- Third parties
- Law enforcement
- Regulatory authorities
- Insurance carrier



Responding: Note on Notification #2

It is not just about PII / financial information anymore

- CA SB1386 was amended to include “medical information” and “health insurance data”
- Sections of the *American Recovery and Reinvestment Act 2009* provide grants and payment incentives for organizations to adopt and make meaningful use of technology designed to create and manage electronic health records (“EHR”s)
- Along with the grants and payment incentives, the legislation includes provisions intended to shore up public confidence in the use of EHRs and personal health records (“PHR”s) by **beefing up enforcement of and expanding the scope of businesses covered by the *Health Insurance Portability and Accountability Act of 1996* (“HIPAA”) Privacy and Security Rules**
- It is somewhat complex and implementation dates vary but this includes expansion of the HIPAA rules and entities that fall under the rules, compliance audits, breach notification and civil and criminal penalties



Responding: Containment and Recovery

Containment and isolation

- Determine when to stop investigation, and when to start containing/controlling
- Take appropriate steps to contain and control the incident to prevent further loss or harm while preserving records and other evidence for further investigations

Recovery

- Take measures to address and mitigate any harm realized by the company, customers and partners

Worth Noting:

- Recognize a practical 'dead end' / point of diminishing returns
- Recovery from technical vulnerabilities may require vendor support, significant programming or significant security configuration
- Recovery may be a multi-phase process as you start with temporary fixes and work your way toward permanent remediation
- This effort is probably not in your budget – impact can be significant



Responding: Post Mortem

Post mortem analysis

- Determine root cause of incident, and determine appropriate mitigating actions
- Review the specifics of this response
 - Identify lessons learned
 - Improve response process
 - Update training program
 - Update threat/risk assessment if appropriate

Practice does not make perfect...but it does make better

Worth Noting:

- Many organizations will get 90% of the way done, then get distracted by day-to-day activities – and the post mortem never happens



Breach Scenario #1



Breach Scenario #2



Breach Scenario #3



Contact Information

Kieran Norton
Senior Manager
Deloitte & Touche LLP
kinorton@deloitte.com

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this presentation.

About Deloitte

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

Copyright © 2009 Deloitte Development LLC. All rights reserved.

