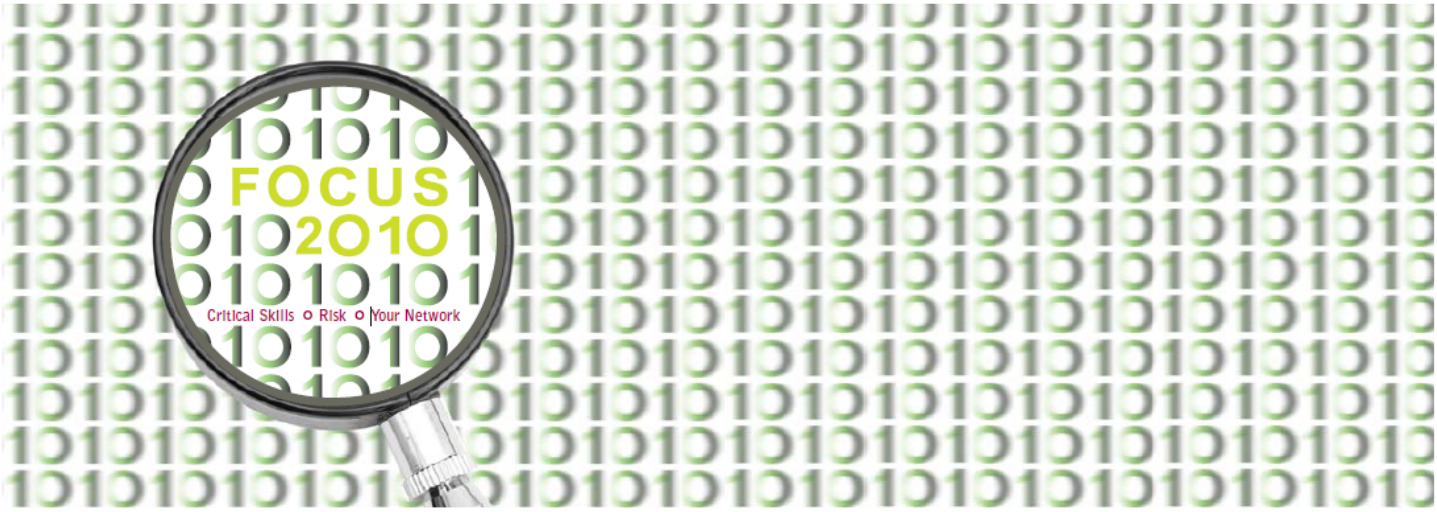
10th Annual SF ISACA Fall Conference

October 4 – 6, 2010



T11: Incident Response Clinic

Kieran Norton, Deloitte & Touche

ISACA®

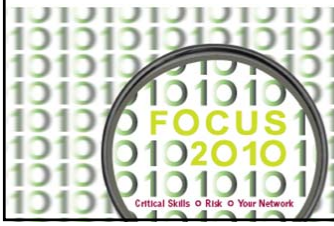
Trust in, and value from, information systems

San Francisco Chapter

ISACA
Trust in, and value from, information systems
San Francisco Chapter

Incident Response Clinic

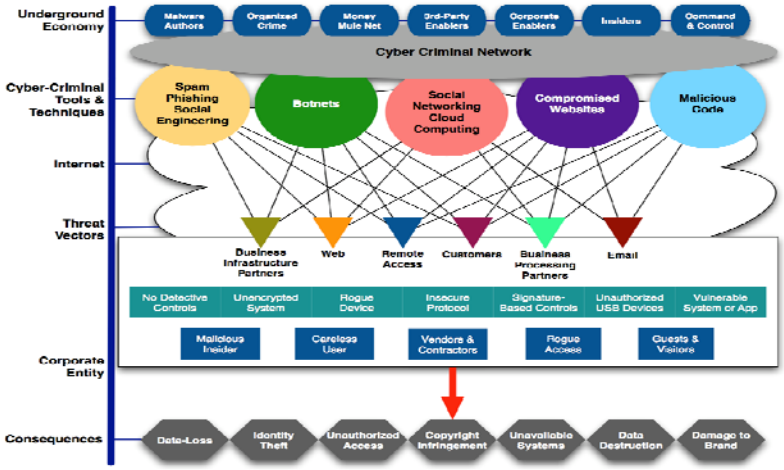
Kieran Norton
Senior Manager, Deloitte



First Things First

- Who am I?
- Who are you?
- Together we will:
  - Review the current landscape and common challenges
  - Outline best practices in developing an incident response program
  - Review the primary steps in the incident response process
  - Walk through 3 - 4 incident response scenarios (interactive)

The Threat Landscape



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

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

Reasonable security program standards / rules

- Forces focus on holistic approach
- Calls for incident response program
- Program must be documented, risk based, part of infosec program
- The yard stick by which you will be measured if you have a breach

Federal Action / Consent decrees

- "Do what you say you do"
- Oversight
- Known vulnerabilities

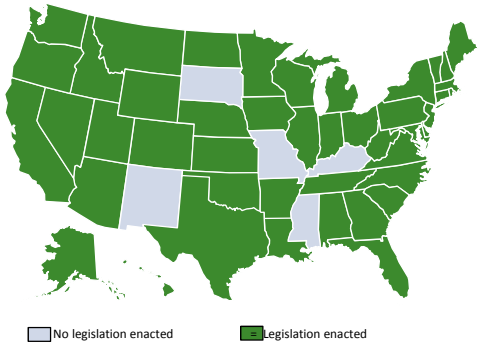
Private Actions

- 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.



Common Challenges

In assisting clients dealing with breaches, we have noticed a few common challenges:

- 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?

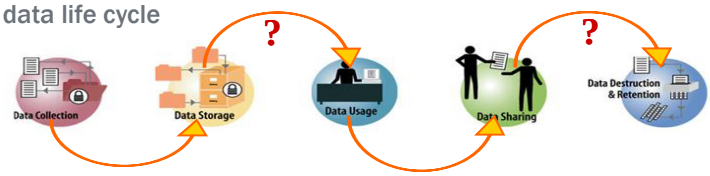
Incidents can take many forms, not all will involve customer data or notification requirements, but all must be dealt with and the line between them is continuing to blur:

- 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 response, the material applies to all of the above and a strong incident response program will deal with multiple incident types

Incident Response Program

- Your IR program should be part of your 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.)

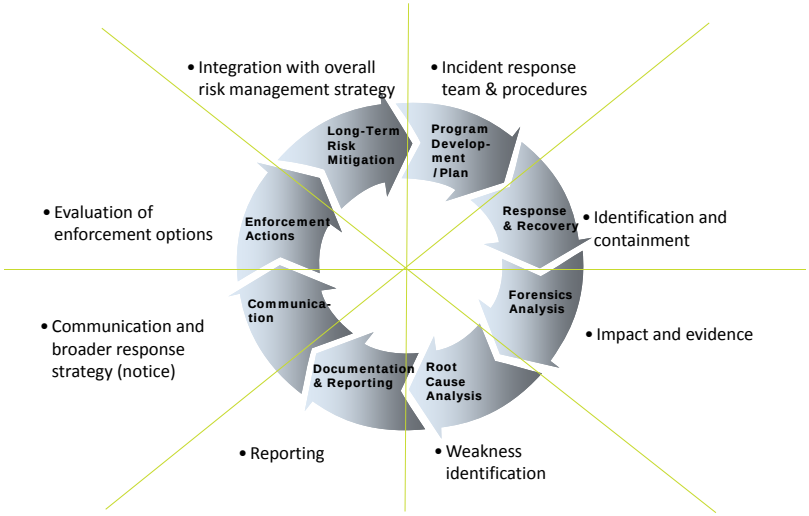
- Early issue spotting is critical:
  - Lost data may have the same consequences as a hacking incident
  - Notice (who to tell, what to tell and when) may not be simple
  - Duties and obligations may not be clear and might conflict (customers, partners, regulatory agencies, law enforcement)
- Post-incident 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
- Establishes the foundation for legal or civil action against perpetrators
- Provides accurate reports and recommendations for improvement

Incident Response Overview



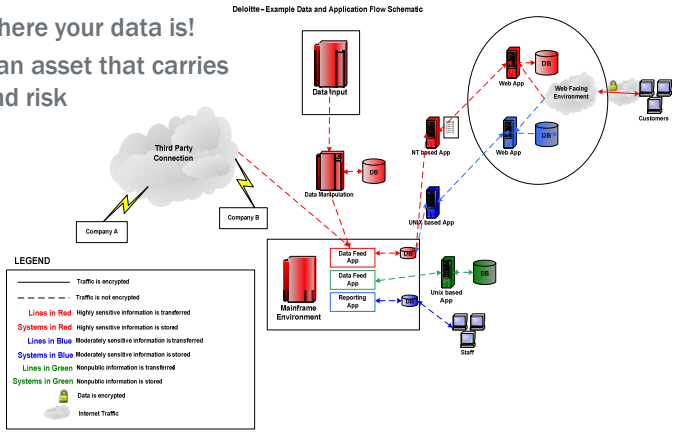
Responding to Incidents: Pre–Incident Preparation

- **Roles and communications 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**

IR Tools:
Have your toolkit ready to go and update it on a monthly or quarterly basis

Responding to Incidents: Pre-Incident Preparation (Cont.)

- Know where your data is!
- Data is an asset that carries value and risk



Responding to Incidents: Investigation

Investigation:

- Obtain basic facts and establish the circumstances (question what you learn)
- 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:

- Be calm and assertive – stress and panic are contagious
- Logging and monitoring is critical to be able to *detect and scope* a breach – too often clients find that they don't have sufficient logging in place when they need it most
- Many of the breaches we have responded to 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 to Incidents: 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 must 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
- Beware the Gonzalez Effect

Responding to Incidents: 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 to Incidents: Another Note On Notification

It is not just about PII / financial information anymore

- CA SB1386 was amended to include "medical information" and "health insurance data"
- The sections of the American Recovery and Reinvestment Act 2009 known as The Health Information and Clinical Health Act 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, but this includes:
  - Expansion of the HIPAA rules
  - Compliance audits
  - Breach notification
  - Civil and criminal penalties

Responding to Incidents: Containment & 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
- Recovering 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 or on your list of projects – impact can be significant

Responding to Incidents: 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 the day by day – and the post mortem never happens

Breach Scenario #1

Breach Scenario #2

Breach Scenario #3

Contact Information

Kieran Norton
Senior Manager
Deloitte
kinorton@deloitte.com
415-783-5382