ISE North America Leadership Summit and Awards

Nominee Showcase Presentation

October 27- 28, 2010

Company Name:	Commonwealth of Massachusetts
Project Name:	**201 CMR 17.00 ID Theft Regulation** – *One of the Toughest ID Theft Regulations in the Country*
Presenter:	Gerry Young
Presenter Title:	Chief Technology Officer (CTO), Public Consulting Group

TEN TECH EXEC NETWORKS

Massachusetts Overview

- List of key company attributes:
- Delivers goods and services to ~ 6.6 million residents … Sometimes does it efficiently!
- 90,000 employees
- $27 Billion/Yr
- Global footprint
- 140 State agencies organized into 8 secretariats

Presentation/Project Overview

- Overview of the Business Challenge
- Background to the Regulation
- Political Challenges (Consumer Affairs & AG)
- Components of the Regulation
  - Written Information Security Plans (WISP)
  - Technical Requirements (Not just IT-Related)
- Approach Taken
- Project Results

Overview of Business Challenge

- In the wake of TJX data breach in 2007, Massachusetts Legislature directed formulation of the regulation (201 CMR 17.00). Minimum Standard.
- *Goal was to protect the **Personal Information** of all Massachusetts residents.*
- ***Personal Information was defined as: First Name (Initial) and Last Name - Plus-***
- ***SSN***
- ***Driver's License Number (or state-issued ID), or***
- ***Financial account number or credit/debit card (with or without pin, password, etc.) that would permit access to a Massachusetts resident's financial account.***

Background to the Regulation

- **Exhaustive search of comparable regulations in other states.**
- **Tried to close the loopholes around:** "own, license, receive, store, maintain, process or otherwise have access to" language.
- **Chapter 82 of The Acts of 2007**
  - **Created MGL Chapter 93H**
    - **Section 2 – Directed OCABR to promulgate regulations**
    - **Section 3 – Breach Notifications**
  - **Created MGL Chapter 93I**
    - **Section 2 – Destruction of documents containing PI**

Political Challenges

- Legislature in Massachusetts tasked Office of Consumer Affairs and Business Regulation to Promulgate the regulation.
- Only the Attorney General's Office has enforcement authority, but no people!
- It became a lobbying nightmare.

201 CMR 17.00

COMPONENTS OF THE REGULATION

Written Info Security Plans (WISP)

- If you own, license, receive, store, maintain, process or otherwise have access to personal information in connection with the provision of goods or services or in connection with employment, you MUST develop, implement, maintain and monitor a comprehensive Written Information Security Plan (WISP)

  - Must be written in one or more readily accessible parts
  - Must contain **administrative**, **technical** and **physical** safeguards
  - At least an annual review process
  - Awareness training

Technical Requirements

- Technical Feasibility
- Secure Authentication Protocols
- Encryption
- Security Monitoring
  - Up-to-Date Firewall
  - Security Patching
  - Malware & Virus Definitions
  - Current Training Program

Technical Requirements (Cont'd)

Encryption:

- Encrypt all PI records and files that are transmitted across public networks, and that are to be transmitted **wirelessly**;
- Encrypt all PI stored on **laptops** or other **portable devices**;
- Note … Type of encryption still not specified

- Best Practices are Best Practices.
- You are only as strong as your weakest link.
- Threats are blurring the traditional lines internal-DMZ-external.
- Focus needs to cover Internal, as well as External threats (People, Process, and Technology).
- Look at your entire security model: Laptops, PDAs, Smartphones, Thumbdrives, Firewalls, IDS/IPS, DNS Servers, Routing & Switches, Authentication models, server hardening, etc. Whole disk encryption?
- Are you using Honeypots (traps) in your DMZ? Full-Duplex Taps? BlackHoles?
- Have you set up Trusted Domains so you can limit damage when you are breached, not if?
- What condition is your Patch Management and Antivirus/Malware?
- What about Personal Information in your Database Tables?

Approach Taken

- Enterprise Security Board (ESB) at the Commonwealth level that drove ISO 27001/27002 adoption led by CISO Dan Walsh
- General Counsel David Murray and I did tag team around state speaking to every group that would have us (legal/technical); podcasts; webinars, industry/legal forums, chambers of commerce, etc. 2008 through 2010.
- IEEE, Society of Information Management (SIM), and other Technology user groups.

Project Results

- Open Security Foundation DataLossDB.org, ITRC, etc. showed a spike in incidents and number of records breached growing from 2007 to 2008 (Incidents - 35%, Records - 211% **171M to 360M**).
- ITRC Report (1/6/10) lists 2009 stats at **222.5M** records.
- Comparable stats in Massachusetts showed a decline in records from **800K to less than 400K**.

Lessons Learned/Best Practices

- Use a broad-based communication strategy
- Business, technology, and government involvement
- Be realistic about the nature of the security threat without being alarmist

Thank you and Questions

- Questions?