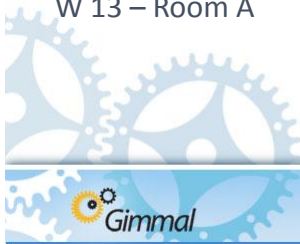


# DEVELOPING AN INFORMATION SECURITY POLICY AND CLASSIFICATION SCHEME

Wednesday, April 29, 2009 8:30 – 9:45 a.m.

W 13 – Room A

Sandy Miller, CRM, McDermott Incorporated  
Susan Cisco, PhD, CRM, FAI, Gimmel



## AGENDA

- Introduction
  - Laws, Regulations, and Standards
  - Third Party Contracts
- Practical Application
  - Background
  - Program
- Benchmark Study for Industry Best Practices



## LAWS AND REGULATIONS – UNITED STATES

- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Trade Commission
  - Fair Credit Reporting Act (FCRA)
  - Fair and Accurate Credit Transactions Act (FACTA)
- Massachusetts 2-1 CMR 17.00



## LAWS AND REGULATIONS – UNITED STATES

- HIPAA
  - Limits use and disclosure of individually identifiable health information (PHI)
    - Includes information created or received by an employer related to the health care of an employee or retiree
  - Employers must proactively safeguard healthcare-related information
    - Includes establishing an approach for identifying healthcare-related information and specifying who may access the information, and the conditions of access



## LAWS AND REGULATIONS – UNITED STATES

- Federal Trade Commission
  - Fair Credit Reporting Act (FCRA)
    - Employers may use consumer credit reports when hiring new employees and when evaluating employees as long as the company is in compliance with the FCRA
    - Before obtaining a credit or background report for employment purposes, company must notify the individual in writing that a report may be used
    - Company also must get the person's written authorization before requesting a credit report



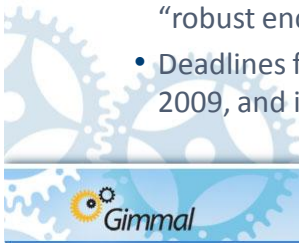
## LAWS AND REGULATIONS – UNITED STATES

- Federal Trade Commission
  - Fair and Accurate Credit Transactions Act (FACTA)
    - If a company uses a credit report for business purposes, it is subject to the requirements of the Disposal Rule, a part of FACTA
    - Disposal Rule requires disposal practices that are reasonable and appropriate to prevent the unauthorized access to or use of information in a consumer credit report



## LAWS AND REGULATIONS – UNITED STATES

- Massachusetts 2-1 CMR 17.00
  - Regulation applies to companies which, “own, lease, store, or maintain personal information about *Massachusetts residents.*”
    - Establishes written policies and procedures for protection of these files, both in electronic and physical formats
    - Ensures that any electronic communication of protected data, whether wireless or online, be conducted using “robust encryption”
    - Deadlines for compliance have been postponed to May 1, 2009, and in some cases, to January 1, 2010



## LAWS AND REGULATIONS - INTERNATIONAL

- Asia Pacific Economic Cooperation (APEC) Privacy Framework
- European Union (EU) Directive 95/46 EC
- Canada Federal Personal Information Protection and Electronic Documents Act (PIPEDA)
- Mexico



## LAWS AND REGULATIONS - INTERNATIONAL

- APEC Privacy Framework
  - 21 member economies in Asia Pacific Region
  - Principles-based framework was adopted in October 2004
  - Current emphasis is on a number of linked Pathfinder projects
  - Work in progress



## LAWS AND REGULATIONS - INTERNATIONAL

- European Union (EU) Directive 95/46 EC
  - Protects against unauthorized processing or transfer of personal data relating to an identifiable individual
  - Data may *only* be transferred to another country if that country provides an adequate level of protection.
  - For countries like US whose privacy practices are not deemed "adequate," US Department of Commerce and European Commission have developed a "safe harbor" framework



## LAWS AND REGULATIONS - INTERNATIONAL

- Canada Federal Personal Information Protection and Electronic Documents Act (PIPEDA)
  - Applies to personal information an organization collects, uses, or discloses in the course of commercial activities or that is about an employee
  - Purpose is to establish rules to govern the collection, use, and disclosure of personal information in a manner that recognizes the privacy rights of individuals



## LAWS AND REGULATIONS - INTERNATIONAL

- Mexico
  - Does not have a privacy/information security law although there are currently 7 different privacy bills active in the Mexican federal legislature
  - Two of the bills are considered front runners:
    1. Bill includes EU data protection mechanisms
    2. Bill based on Organization for Economic Cooperation and Development (OECD) Privacy Guidelines and APEC Privacy Framework and is consistent with PIPEDA and US regulatory approaches



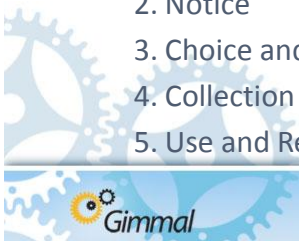
## STANDARDS

- Generally Accepted Privacy Principles (GAPP)
- ISO/IEC 2700 Series
- Payment Card Industry Data Security Standard (PCI DSS)
- Standard of Good Practice for Information Security



## STANDARDS

- **GAPP (Generally Accepted Privacy Principles)**
  - Developed by American Institute of Certified Public Accountants & Canadian Institute of Chartered Accountants - AICPA/CICA Privacy Task Force
  - Provides privacy principles for maintaining customers' personal information:
    1. Management
    2. Notice
    3. Choice and Consent
    4. Collection
    5. Use and Retention
    6. Access
    7. Disclosure to Third Parties
    8. Security for Privacy
    9. Monitoring and Enforcement
    10. Quality



## STANDARDS

- ISO 27000 Series
  - Similar in design to management systems for quality assurance (ISO 9000 series) and environmental protection (ISO 14000 series)
  - Information Technology - Security Techniques - Code of Practice for Information Security Management  
ISO/IEC 27002:200 emphasizes:
    - Preservation of confidentiality
    - Integrity
    - Availability



## STANDARDS

- PCI DSS
  - Applies to organizations that store, process, or transmit credit card holder data
  - Is a contractual obligation applied and enforced by means of fines or other restrictions directly by the payment providers themselves
  - Requirement 12 - Organizations must have policy that addresses information security
  - Minnesota has codified various parts of PCI DSS into law & other states are considering similar legislation



## STANDARDS

- Standard of Good Practice for Information Security
  - Revised every 2-3 years by the Information Security Forum, an international association of organizations
  - Complying with the standard can help organizations conform with other information security-related standards, such as ISO/IEC 27002 and PCI DSS
  - Standard is split into the 6 key areas of security management from laptop encryption to end user training



## THIRD PARTY CONTRACTS

- Third parties (suppliers and vendors) contracted to administer payroll, manage employee benefits including health plans, conduct background checks, etc. must be required to comply with company's information security policies
- Your company's contracts with customers are likely to mandate information security requirements



## DEVELOPING AN INFORMATION SECURITY POLICY

### Q&A



## BACKGROUND

- Information Security – Definition
  - The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.



- Source: Glossary of Key Information Security Terms, National Institute of Standards and Technology  
[http://csrc.nist.gov/publications/nistir/NISTIR-7298\\_Glossary\\_Key\\_Infor\\_Security\\_Terms.pdf](http://csrc.nist.gov/publications/nistir/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf)



## BACKGROUND

- Information Security – Historical Perspective



**C. 50 BC** - Julius Caesar's invention of the Caesar Cipher for secret communication



**WWII** - Many advancements in the field were introduced during World War II



**1990's- Present** - Greatest advancements achieved in this period



## BACKGROUND

- The core principals of information security have been referred to as the CIA Triad

Confidentiality – Preventing disclosure and unauthorized use

Integrity – Inability to modify information without authority

Availability-Availability of information when needed



## BACKGROUND

- Security Cost Estimates (Year 2005)
  - Industry Security Classification 1.5 billion
  - Government Security Classification 7.7 billion

Source: The National Archives Information Security Oversight Office (ISOO)  
<http://www.archives.gov/isoo/reports/2005-cost-report.html>



## PROGRAM

- Business Purposes
  - RIM polices/procedures provide for necessary security
  - Compliance
  - Risk Reduction
  - Protect Intellectual Property



## PROGRAM

- Business Purposes (continued)

- Reputation Damage

*"The problem with e-mail has often been that one person will say, well, I'll just forward that to one more person, and that person forwards it to another person and so on until it's on the front page." (Bill Gates)*

- Cost Savings

- Efficiencies

Source: RSA Conference

<http://www.microsoft.com/Presspass/exec/billg/speeches/2007/02-06RSA.mspx>



## PROGRAM

- What actions should be taken?

- Policies/Procedures
  - Classification Scheme



## PROGRAM

- Develop Policy/Procedures & Classification Scheme
  - Approach
    - Review existing policies/procedures
      - Corporate-wide scope
      - Records & Information Management
    - Subject Matter Expert (SME) interviews
      - Disciplines to interview
    - Partner with Information Technology



## PROGRAM

- Develop Policy/Procedures
  - Considerations
    - Include Classification Scheme matrix as an appendix
    - Include direct references in the Records Retention Schedule



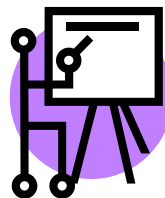
## PROGRAM

- Develop Classification Scheme
  - Considerations
    - Develop Matrix
      - Determine number of levels
      - Specify controls mandated
        - Include hardcopy, electronic, removable media



## PROGRAM

- Examples
  - Searching the internet will provide a variety of approaches
    - Examples are often in the form of a Matrix for ease of use



## PROGRAM

- Develop Classification Scheme (Continued)
  - Matrix - must be unique to company and take into account
    - Corporate Culture
    - Type of industry
    - Risk
    - Availability of technology solutions



## DEVELOPING AN INFORMATION SECURITY POLICY

### Q&A



## BENCHMARK STUDY

- Benchmark Study for Industry Best Practices
  - Private sector
  - Public sector
    - By industry sector



## CONTACT INFORMATION

- |  |  |
|--|--|
| • Sandy Miller, CRM  | • Susan Cisco, CRM   |
| • McDermott International  | • Gimmel Group   |
| • <a href="mailto:srmiller@mcdermott.com">srmiller@mcdermott.com</a> | • <a href="mailto:susan.cisco@gimmel.com">susan.cisco@gimmel.com</a> |
| • 281-870-5593   | • 512-565-7021   |



**THANK YOU**

---

**Q&A**

