Creating a Proven Data Protection Strategy

Russell L. Jones, Partner
Deloitte & Touche LLP
AERS – Security & Privacy Services
Key Questions

- Do we know what data is critical, when it is critical, and where it is?

- Do we know who is accountable for it (who owns it and/or controls it)?

- Do we know how it is used and how it should be restricted?

- Do we know how to protect it while enabling its effective use?
• Defining the Problem Space
• Enterprise Data Protection: Pre-requisite Work
• Defining Data Protection Requirement Sources
• Creating the Enterprise Data Protection Framework
• Creating The Enterprise Data Protection Strategy
• Questions & Answers
Data as an asset

Data is an asset with multiple attributes. The value associated with data is determined by its attributes, context within the enterprise, and associated risk.

The nature of data changes over time, as it is stored, used and shared.
Problem Statement
How do you protect/control the data once it is outside the boundaries of your organization?
Enterprise Data Protection: Pre-
Enterprise Data Protection: Pre-

Key Questions:

1. **What** is the data (e.g. IP, PII, Financial, etc..)?
2. **Where** is the data?
3. **How** is the data used and by whom/what?
Pre-requisite Work

- Data classification policy (*What?*)
- Data and business process flow diagrams (*Where?, How?*)
3 – 4 categories should be sufficient

- Public
- Confidential
- Confidential-Restricted

Hopefully, data mapping exists between the business and applications/infrastructure

Input into enterprise data protection framework development
Where is the Data?

Data Category
- Intellectual Property
- CPNI
- Sensitive Financial
- PII
- Etc..

Data Type
- Structured vs. Unstructured

Risk Factors
- Internal threats
- External threats
- Value
- Brand
- Etc..

Data Integrity
- Schema
- Meta data

Business Process Areas
- Order-to-Cash
- Procure-to-Pay
- Engineering
- Legal
- Etc..

Data Triage Logic

Data Triage
- Order-to-Cash
- Procure-to-Pay
- Engineering
- Legal
- Etc..

Data Type
- Structured vs. Unstructured

Risk Factors
- Internal threats
- External threats
- Value
- Brand
- Etc..

Data Integrity
- Schema
- Meta data
Defining Data Protection
Defining Data Protection Requirement Sources

- What is your “universe” of data protection requirements?
Defining Data Protection Requirement Sources

- To determine "universe" of requirements, each organization needs to consider:
  - All geographic locations of the organization
    - E.g. HQ in Chicago, sales offices in UK and France, manufacturing operations in Dallas
  - Industry affiliation
    - E.g. financial services, life sciences, high-tech, etc...
  - Regulatory requirements
  - Legal requirements
  - Contractual requirements
  - Data protection standard(s)

These parameters are inputs that define all of the data protection requirements
Requirement Sources

Example: Multi-national life sciences organization

- HQ – Los Angeles, Calif.
- U.S. operations in:
- International operations in:
  - UK, France, Spain
  - Singapore, Tokyo
Defining Data Protection Requirement Sources

Example: Multi-national life sciences organization

- **Int'l Laws**
  - EU Data Protection
  - Member State Laws - UK, France, Spain
  - APEC Privacy

- **Industry Regulations**
  - FDA 21 CFR Part 11
  - HIPAA

- **State Laws**
  - CA - SB 1386
  - CO - HB 06 1119
  - WA - SB 6043

- **Contractual**
  - Confidentiality

- **Data Protection Standards**
  - ISO 17799:2005
  - AICPA/ CICA
  - NIST 800-53
  - PCI DSS ver 1.1
Protection Framework

- Three Step Process
  1. Select industry leading standard as basis of the enterprise data protection framework
  2. Rationalize identified requirements against preferred standard
  3. Vet enterprise data protection framework with stakeholders
Developing A Controls Framework

- Administrative
- Organizational
- Technical
Protection Framework

- With the enterprise data protection framework, you can now:
  1. Perform a gap analysis of existing data protection controls
  2. Develop a strategy and roadmap for enterprise data protection program implementation and gap remediation
Gap Analysis and Strategy

Data Discovery Results

Data Protection Framework

Gap Analysis

Strategy & Roadmap
Enterprise Data Protection Strategy & Roadmap

Phase 1
1.1: Laptop Encryption Pilot
1.2: Enhance Data Protection Policy & Procedures

Phase 2
2.1: Enterprise Laptop Encryption Deployment
2.2: Enhance Data Classification Scheme

Phase 3
3.1: Enterprise PKI I
3.2: Enhance Enterprise Web Access Control
3.3: Enterprise Rights Management Pilot

Phase 4
4.1: Enterprise Role Mgt Pilot
4.2: Enterprise Rights Management Rollout
4.4: Expanded Enterprise PKI II

Phase 5
5.1: Enterprise Role Mgt Rollout
5.2: Privacy Enhancing Technology Vendor Selection Project

Example - Enterprise Data Protection Roadmap