Leave it to the experts
How to implement and manage Data Loss Prevention

Matt Adams
15 November 2012
Introduction

Joined Deloitte in 2006

Service Lead – Information Protection Technologies

- DLP
- Data classification
- Mobile security

CLAS, CISSP, CISM, ISO 27001 Lead Auditor
Agenda

• Introduction to Deloitte Information Protection Technologies
  – Observed trends
  – Capabilities

• DLP Case Study
  – Stakeholder engagement
  – Project approach
  – Lessons learned

• Partnering summary

• Q&A
Information Protection Technologies
Service Overview
Information Protection Technologies

What we’re seeing...

• Organisations have deployed a range of ‘point solutions’ designed to protect sensitive information.

• Key challenge to ensure these solutions deliver ongoing business value and secure business data.

• Point solutions can be difficult to integrate to achieve ‘defence in depth’.

• Effectiveness of solutions can be eroded over time if configurations and rule sets are not maintained.

• Resource limitations can prevent organisations from realising the full benefits of solution capabilities and reporting.
Information Protection Technologies

How are we helping our clients...?

• Team of information protection specialists, certified by leading vendors.

• Focussing on maximising the business value of existing and planned implementations of information protection solutions.

• Leveraging combined experience of delivering projects for other leading organisations.

• Combining technical SME’s with knowledge and insight from business representatives.

• Providing access to our Information Protection Laboratory for demos and testing.
Deloitte Information Protection Lab

Internal network – Information Protection Lab – LAN Address

Shared Services Infrastructure
- MS Exchange 2010
- MTA
- SharePoint 2010
- File Server
- Active Directory

Same virtual box

Workstations/clients
- Titus client
- Symantec DLP client

Information Protection
- Oracle IRM
- DLP Vendors
- Varonis
- PGP Universal (SMTP Gateway)

Shared Database Services
- Oracle Database
- MS SQL 2010

Workstations/clients
- Oracle IRM client
- Varonis

Leave it to the experts: How to implement and manage DLP
Symantec Data Loss Prevention
Client case study
## Engagement Overview

<table>
<thead>
<tr>
<th>Client Profile</th>
<th>Deloitte Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Leading multi-channel media company.</td>
<td>• Identify sensitive business data and associated business users.</td>
</tr>
<tr>
<td>• National and regional newspaper titles plus a</td>
<td>• Account for changes in data flows as a result of cloud and consumer device</td>
</tr>
<tr>
<td>portfolio of more than 200 websites.</td>
<td>initiatives.</td>
</tr>
<tr>
<td>• Part of a global B2B and consumer media group.</td>
<td>• Lead workshops with business stakeholders.</td>
</tr>
<tr>
<td></td>
<td>• Perform a DLP risk assessment against existing practices and controls.</td>
</tr>
<tr>
<td></td>
<td>• Produce high-level technical design.</td>
</tr>
<tr>
<td></td>
<td>• Manage a phased deployment of network and endpoint DLP, data classification</td>
</tr>
<tr>
<td></td>
<td>and information rights management technologies.</td>
</tr>
</tbody>
</table>
Managed DLP Deployment

- Business Enablement (Deloitte)
- Technology Vendor (Symantec)
- Managed Services Provider

Managed DLP
Project Stakeholders

1. Client Project Lead
2. Deloitte Project Team
   - Technology Vendors
   - Managed Service Provider
3. Business Unit Reps
Project Outline - DLP

05/11 DLP Risk Assessment
07/11 Phase 1 (Passive)
10/11 01/12 04/12 07/12

Phase 2 (Active)

Network Monitor for Email and Web
Network Prevent for Email and Web
Endpoint Discover
Endpoint Prevent
Risk Assessment

Objective

Identify whether there is an issue with data leakage from business systems and determine possible causes.

Approach

• Deploy Symantec DLP Risk Assessment tool to scan outbound emails, including attachments.
• Tailored search criteria developed by Deloitte in collaboration with client IT Risk team and business representatives.
• 5,000 email addresses monitored.
• Four consecutive weeks.

Results

• Identified a large number of significant breaches of the Data Protection Act.
• Observed a range of company confidential documents being sent to external email addresses.
• Recommended improvements for remote working and information sharing with third-parties.

Leave it to the experts: How to implement and manage DLP
Phase 1 – Passive Monitoring

Business Unit Workshops
Understand business context of sensitive data processing. Identify business requirements.

Define Business Processes
Analyse output from workshops and agree what ‘normal’ looks like.

Create Policies / Rule Sets
Specific rules for each business unit.

Design DLP Infrastructure
Deloitte collaborated with client IT personnel and managed service provider to identify optimum network locations to deploy DLP.
Deloitte provided input based on good practice in other leading organisations.

Define Target Operating Model
Deloitte provided a technical review of the tool, presenting results to business unit reps for feedback.

Test DLP Tool
Iterative process of reviewing DLP output and refining rules to optimise output.

Go Live
Phase 2 – Active Monitoring

**Business Unit Workshops**

Gain feedback from key stakeholders.

**Further Policy Refinement**

Update baseline policies and define additional baseline policies for web monitoring.

**Tool and Policy Testing**

Creation of test plan and scripts, including updated baseline email / web policies and response rules.

**Refine Target Operating Model**

Update Target Operating Model with workshop input from key stakeholders.

**Alerting Testing**

Configuration and testing of DLP alerting and messaging workflow.

**Alerting Go Live**

Continue to update and refine rule sets.

Transition to BAU.
DLP Essentials

Ensure business defines teams / employees to be monitored
Overall project sponsorship should come from the business, not IT
Identify key risks with business units
Don’t be tempted by a ‘catch-all’ approach

Think about worst case scenarios
Let the business define keywords and key phrases for monitoring
Ensure regular processes that may trigger DLP are accounted for
Define a clear target operating model

Plan your incident remediation strategy
Consider engaging an experienced delivery partner
Partnering for success
Partnering for greater value

CLIENT CHALLENGES
- Point solutions
- IT focus
- Sustaining value
- Resource constraints

DELOITTE VALUE
- Strategic vendor partnerships
- Industry knowledge
- Significant implementation experience
- Flexible pool of SMEs

Leave it to the experts: How to implement and manage DLP
Why Deloitte?

- We are a global strategic partner with leading vendors of information protection technologies
- Symantec Security Partner of the Year 2012 (EMEA)
- Enterprise Solution Provider for Symantec DLP
- Wealth of experience in supporting clients to deploy and manage solutions throughout the information protection lifecycle, including:
  - Data Loss Prevention
  - Data Access Governance
  - Data Classification
  - Data Encryption
  - Information Rights Management
  - Mobile Device Management
Why Deloitte?

Our security and IT risk consulting services are independently recognised as world leading.

“In Forrester’s 75-criteria evaluation of information security and risk consulting service providers, we found that Deloitte led the pack because of its maniacal customer focus and deep technical expertise.”

Our people

At Deloitte, our global team can draw on the experience of:

• 11,000 risk management and security, privacy and resilience practitioners
• 16,000 risk consulting professionals
• 210 computer forensics examiners
• 11,530 human capital consulting professionals

Our skills

✓ ISACA: Over 8,000 involved with ISACA; approximately 2,000 certified as CISA, CISM, & CGEIT
✓ ISC²: Over 1,100 CISSPs
✓ BSI: 150 trained lead system auditors
✓ IAPP: Privacy certified practitioners
✓ PMI: PMP certified practitioners

53 Security & Forensics labs located strategically across the globe
Questions?

Please feel free to ask questions now, or get in contact with me through the following addresses.

Email: mattradams@deloitte.co.uk
Twitter: @mattrwa

Alternatively, please come along to the Deloitte stand (PL1) in the Expo Hall.