Leave it to the Experts:
How to Implement and Manage Data Loss Prevention

Rob Eggebrecht
President/CEO, BEW Global

Jerome Quiroga
CTO, ATSccloud
BEW Global & ATS Key Milestones

- 2005: ATS become BEW Global customer
- 2006: ATS deployed Symantec DLP
- 2008: BEW Global commenced management of ATS DLP system
- 2010: ATS launched ATSccloud
  - ATS migrated Cardiology practice to the ATSccloud
- 2011: BEW Global & ATSccloud partner for cloud DLP
- Q1 2012: Cloud DLP deployed for Cardiology practice
  - First Beta Customer
### Use Case: DLP Pre-Project State

<table>
<thead>
<tr>
<th><strong>Organization Overview:</strong></th>
<th>Cardiology Practice: 700 Employees, 25 Locations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DLP Scope:</strong></td>
<td>Protection of PHI, PII, PCI – Card Data</td>
</tr>
<tr>
<td><strong>DLP Primary Issue:</strong></td>
<td>Customer overwhelmed with incident data, numerous false positives.</td>
</tr>
<tr>
<td><strong>Application Management:</strong></td>
<td>Operated and managed by IT with limited input from business.</td>
</tr>
<tr>
<td><strong>Policy Governance:</strong></td>
<td>Using out of box policies, limited modification. No finger printing.</td>
</tr>
<tr>
<td><strong>Incident Triage:</strong></td>
<td>Infrequently reviewed by IT with little to no review by business owners.</td>
</tr>
<tr>
<td><strong>Event Management:</strong></td>
<td>Driven by high match counts. Typical “shock value” mentality.</td>
</tr>
<tr>
<td><strong>Reporting and Metrics:</strong></td>
<td>Relies on pre-built in system reporting with no correlation analysis.</td>
</tr>
<tr>
<td><strong>Status:</strong></td>
<td>Over 3M incidents interface. Cannot start user notifications.</td>
</tr>
</tbody>
</table>
Data Loss Prevention Quality Management Approach

- Incident Triage
- Scope & Policy Governance
- Application Management
- Reporting & Metrics
- Application Management
- Policy Governance
- Incident Triage & Event Management
- Reporting & Key Performance Metrics

How to Implement and Manage DLP - BEW Global & ATSccloud
Application Support & Integration

Primary System DLP Management = Resource Requirements
Integrated System Management = Cross Department Processes
Upgrade & Release Management = Resource Requirements
Vendor Management = Primary and Integrated Technology Vendor Relationships

How to Implement and Manage DLP - BEW Global & ATScloud
Policy & Rule Governance

Who requests rules & policy requirements?
Are business owners engaged?

Who reviews rule requests?
Criteria for approved rule?

What’s the process for converting a rule request into a policy?

Is there a process to relay production policy metrics?

What is the formal policy development process?
First drafts rarely work as expected.

Who’s responsible for converting a rule into technical policy?
Do they policy building expertise?
Workflow Development & Management

Who develops & manages policy “buckets”?  
False positive, inbound partner, outbound employee

Who defines thresholds that determine response rules for each “bucket”?  
Are 10 SSNs a high, medium or low severity incident?

Who designs & sets the policy response triggers?  
Malicious, Inadvertent, Suspicious, above threshold.

Triage response options:  
- Human notification  
- System notification (auto)  
- Hybrid?

Who’s responsible for building alerts, alarms & notifications?  
Has business been engaged on event management?

Who manages the DLP policy & rules repository?  
Why recreate the wheel?

How to Implement and Manage DLP - BEW Global & ATScloud  
SYMANTEC VISION 2012
Incident Triage & Event Management

Who reviews volume & yield of incidents & events?
- What’s the review frequency?

How are events/incidents routed?
- Who owns the incident/event?

How does DLP fit in overall incident/event management process?
- Can this be mapped to DLP system?

What metrics are developed to measure success of rules & related policy?
- Who’s responsible for developing metrics?

Revision of rules based on quality of policy results.
- Who manages policy optimization process?

How will integrated systems be tied together to yield valued info?
- Secure mail, web gateway, GRC, SIEM
Records Retention & Reporting

- What incidents or events are retained?
- How long is the retention period? Regulatory requirements?
- Who develops reports?
- Are DLP system generated reports adequate?
- Who drives report requirements? Requestors, Reviewers, others?
- Report accuracy tied into QA process?
Application Management Pitfall: Inadequately Training Infrastructure Resources

Inadequate Planning & Resources

- **Problem:** Current IT infrastructure management is often inadequately trained for planning, deployment and ongoing operational management of DLP operation system. (Oracle vs. SQL, etc.)

- **Solution:** Outsourced 3rd party management of on premise solution or fully managed cloud-based delivery. This provides you with instance expertise reducing the need for staffing and providing higher availability.
Policy Governance Pitfall: No Plan of Attack

Inadequate Planning & Resources

**Problem:** A survey of 50 DLP customers in 2010 said 83% of firms did not consider the overall DLP system cycle & the necessary resources for optimal system usage prior to solution acquisition. Inadequate or lack of resources leads to poor policy construction & unmanageable incidents.

**Solution:** A well thought out DLP scope with a supporting policy governance process that is **VERY inclusive of business unit** input as well as involvement with the triage & event management process. There must be people budgeted for any DLP project as well as preparation for business unit buy-in.
Policy Governance Pitfall: Failure to Engage the Business

Stuck in the IT Department

• **Problem:** A survey of 50 DLP customers in 2010 said **76%** of firms stated the DLP system technical management & daily operations were the responsibility of a group directly involved with IT. In these cases it is very rare to find heavy involvement from business owners directly involved with the creation & usage of the data targeted for protection.

• **Solution:** Designation of a primary business owner of the DLP solution, in conjunction with technical management, is the best recipe for success on the *front-end planning phase* of the project. Without direct & serious involvement from the business, it is very likely that the entire DLP will never get more than mediocre results.
Policy Governance Pitfall: Lack of Rule Customization

Inaccuracy of Out-of-Box (OOB) Policies

• **Problem:** The reliance of organizations to use OOB policies as the primary detection criteria for their DLP scope. In many cases data identifiers in OOB policies may *never capture unique attributes* of an organization's information targets, yielding a combination of false positives and false negatives which lead to an unmanageable incident yield.

• **Solution:** Prior to enabling *ANY* managed production policies, it is highly recommended to select *one primary data criteria* to focus initial efforts. Once agreed upon, use business process mapping to capture how the data is used and stored, obtain examples, and then construct policies based on the collected data.
### Data-in-Motion Pitfalls: Missing the Target – False Sense of Security

<table>
<thead>
<tr>
<th>Mis-configured Tap or Port Span</th>
<th>Encryption – The Masked Data</th>
<th>Misfire of Network Discovery Scans</th>
<th>Network versus Endpoint Discovery</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Problem</strong> Missing segments of network traffic or protocols</td>
<td><strong>Problem</strong> Analysis of data DID not take place prior to encryption.</td>
<td><strong>Problem</strong> Locations of sensitive data <em>never targeted</em> by the organization for scanning due to lack of an effective policy governance process.</td>
<td><strong>Problem</strong> Running DAR scans using a combo of network &amp; endpoint without thinking about which <em>policy types &amp; detection methods are not the same</em>.</td>
</tr>
<tr>
<td><strong>Solution</strong> Comprehensive test plan that maps to in scope business processes and related data types transmitted from various network locations to ensure all relevant data streams are being captured.</td>
<td><strong>Solution</strong> Comprehensive test plan that proves ALL DLP data assessment takes place prior to the gateway encryption &amp; implement managed “test” DLP policies that identify encrypted transmissions as part of the test plan.</td>
<td><strong>Solution</strong> Identify potential data stores by discussing the DLP program with staff to understand process.</td>
<td><strong>Solution</strong> Prior to acquiring DLP solution, have an understanding of the data types that make up your target environment &amp; then, decide on scanning method.</td>
</tr>
</tbody>
</table>
# Data-in-Use (Endpoint) Pitfalls: The Pandora Box of DLP

<table>
<thead>
<tr>
<th>Environment Assessment</th>
<th>Endpoint Agent Check-in</th>
<th>Endpoint Policy Management - # 1</th>
<th>Network vs. Endpoint Discovery</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Problem</strong></td>
<td><strong>Problem</strong></td>
<td><strong>Problem</strong></td>
<td><strong>Problem</strong></td>
</tr>
<tr>
<td>No rigorous endpoint environment assessment prior to the selection of the application &amp; enablement.</td>
<td>Failure to monitor endpoints population &amp; their frequency of &quot;checking-in&quot; to the management server with validated results.</td>
<td>Implementing same policies for network based &amp; endpoint assessments without testing or modification.</td>
<td>Failure to calculate &amp; measure the impact of endpoint policy traffic across wide &amp; local area network connections.</td>
</tr>
<tr>
<td><strong>Solution</strong></td>
<td><strong>Solution</strong></td>
<td><strong>Solution</strong></td>
<td><strong>Solution</strong></td>
</tr>
<tr>
<td>Address age of environment, performance capabilities, technical &amp; human issues, &amp; load of applications, in conjunction with education on the DLP endpoints.</td>
<td>Phased deployment of endpoint with validation via test plan on initial success of ALL agents &amp; on-going endpoint agent health reports.</td>
<td>Utilize a comprehensive test plan outlining specific metrics (time to open files, open/send emails, open applications) prior to deployment.</td>
<td>Thorough assessment of endpoint policies that addresses all of the concerns including policy design requirements, timing, frequency &amp; delivery methods.</td>
</tr>
</tbody>
</table>
Sample Quarterly Report

- HIPAA (including PHI)
- OCA 1 Attachment B
- OCA 1 Attachment A
- OCA 1 Attachment H
Sample Quarterly Report

High-Level Incident Report - 12-Month Trend

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SSN - Custom # 1</td>
<td>340</td>
<td>365</td>
<td>232</td>
<td>134</td>
<td>122</td>
<td>54</td>
<td>43</td>
<td>34</td>
<td>22</td>
<td>21</td>
<td>19</td>
<td>12</td>
</tr>
<tr>
<td>SSN - Custom # 2</td>
<td>456</td>
<td>512</td>
<td>654</td>
<td>467</td>
<td>345</td>
<td>123</td>
<td>98</td>
<td>75</td>
<td>54</td>
<td>32</td>
<td>30</td>
<td>22</td>
</tr>
<tr>
<td>SSN - Standard</td>
<td>1008</td>
<td>1345</td>
<td>2134</td>
<td>1546</td>
<td>1245</td>
<td>875</td>
<td>774</td>
<td>665</td>
<td>543</td>
<td>223</td>
<td>103</td>
<td>34</td>
</tr>
<tr>
<td>PHI - MRN # 1</td>
<td>104</td>
<td>156</td>
<td>203</td>
<td>192</td>
<td>245</td>
<td>234</td>
<td>154</td>
<td>132</td>
<td>98</td>
<td>32</td>
<td>23</td>
<td>8</td>
</tr>
<tr>
<td>PHI - MRN # 2</td>
<td>98</td>
<td>76</td>
<td>45</td>
<td>86</td>
<td>65</td>
<td>78</td>
<td>65</td>
<td>54</td>
<td>49</td>
<td>22</td>
<td>12</td>
<td>2</td>
</tr>
<tr>
<td>PHI - Billing Code # 1</td>
<td>2345</td>
<td>1367</td>
<td>2678</td>
<td>1876</td>
<td>2589</td>
<td>1457</td>
<td>1398</td>
<td>350</td>
<td>223</td>
<td>103</td>
<td>19</td>
<td>12</td>
</tr>
<tr>
<td>PCI - Credit Card # 2</td>
<td>65</td>
<td>78</td>
<td>98</td>
<td>43</td>
<td>12</td>
<td>8</td>
<td>6</td>
<td>4</td>
<td>3</td>
<td>12</td>
<td>3</td>
<td>9</td>
</tr>
</tbody>
</table>
Thank you!

Robert Eggebrecht
robert@bewglobal.com

Jerome Quiroga
jquiroma@atscloud.com