Contemporary Concepts in Information/Data Security –
Data Loss Prevention, Information Rights Management

Arun Aravindan
COO, Elite Technologies Middle East
Agenda

• Setting the context

• Security and Collaboration

• Data Loss Prevention Technologies

• Comparisons and implementation challenges
Setting the Context – Initial Focus

- Firewalls
- VPN
- IDS
- IPS
- UTM
- SIEM
- VA / PT
- DMZ
- Enterprise
Setting the Context – Trends

*Study by a leading consulting firm

Source of data loss breach

By cause of data loss: Number of records/people affected between June 2007 - June 2010

<table>
<thead>
<tr>
<th>Incident Type</th>
<th>Number of people affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improper disposal</td>
<td>7,77,69,077</td>
</tr>
<tr>
<td>Hard copy theft/loss</td>
<td>1,361,008</td>
</tr>
<tr>
<td>Portable media theft/loss</td>
<td>114,192,269</td>
</tr>
<tr>
<td>PC Loss</td>
<td>5,98,577</td>
</tr>
<tr>
<td>PC Theft</td>
<td>13,852,948</td>
</tr>
<tr>
<td>Hacking</td>
<td>2,49,351,765</td>
</tr>
<tr>
<td>Malicious Insider</td>
<td>23,521,995</td>
</tr>
<tr>
<td>Malware</td>
<td>67,815</td>
</tr>
<tr>
<td>Web / Network Exposure</td>
<td>23,356,796</td>
</tr>
<tr>
<td>Human / System Error</td>
<td>8,297,740</td>
</tr>
<tr>
<td>Unknown</td>
<td>1,352,344</td>
</tr>
</tbody>
</table>

Number of malicious insider incidents as % Total
Setting the Context – Current Focus

COMPETITOR

SUB-CONTRACTOR

Enterprise

WikiLeaks

Competitors
Great – what do we do now?

Risks and Controls:
1. Administrative
2. Technical
3. Physical

Our discussion today is around technical or technology controls

A typical approach most organizations follow is to restrict collaboration methods.

Security at the expense of collaboration
Security and Collaboration

- Passing on critical information to vendors (potential or otherwise) to enable them to bid for projects or undertake projects.
- Critical business information goes to external auditors.
- Some organizations generate revenue through reports sent out externally.
- Organizations who are candidates for a merger/acquisition may end up sharing information with competitors.
- Companies with significant churn in workforce and employees moving to competition.

Share it = It becomes his (also)
Shared Once = Shared Forever
Out of the enterprise = Free for All
Data Loss Prevention Technologies

- Most comprehensive solutions do the following:
  - **Locate and catalogue** sensitive information stored in the enterprise.
  - Monitor and control the movement of sensitive information **across the enterprise networks**.
  - Monitor and control the movement of sensitive information **on end user systems**.

- DLP Technologies are **content aware**.
- This is done within a **boundary / perimeter**.
- Policies need to be **configured**, based on which the systems will identify sensitive information.
- When sensitive information is identified, the system applies controls **configured**.
Typical DLP architecture

Data Security Management Server
- Policy Engine
- Forensics Repository
- Fingerprint Repository
- Describing Repository
- Crawler

Controller
- (Email, FTP, HTTP, Chat)
- Fingerprint Repository
- Describing Repository

End Users

File Servers

Email Server

ISA Server

Agent

Detection Technologies
- Describing
- Fingerprinting
- Vector Machine Learning

Web
Information Rights Management

• Controls are applied by business users on documents created by them though in some cases controls can be forced.
• Once documents are protected, the policies apply irrespective of whether the document is inside the enterprise or outside.

WHO can use the information
People & groups within and outside of the organization can be defined as rightful users of the information

WHAT can each person do
Individual actions like reading, editing, printing, distributing, copy-pasting, screen grabbing etc. can be controlled

WHEN can he use it
Information usage can be time based e.g. can only be used by Mr. A till 28th Sept OR only for the 2 days

WHERE can he use it from
Information can be linked to locations e.g. only 3rd floor office by private/public IP addresses
Typical IRM architecture

- Active Directory
- LDAP
- IRM Policy Server
- Policy Database
- IRM client enabled machines
- Enterprise
- DMZ
- Internet
- Web

IRM client enabled machine
# Comparing DLP and IRM technologies

<table>
<thead>
<tr>
<th>DLP</th>
<th>IRM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What it does</strong></td>
<td><strong>What it does</strong></td>
</tr>
<tr>
<td>Discover the presence of information on heterogeneous systems</td>
<td>Define information usage policy i.e. specifies WHO can use, WHAT can be done, WHEN can information be used &amp; WHERE</td>
</tr>
<tr>
<td>Protect the information by controlling its flow</td>
<td>Implement policy controls</td>
</tr>
<tr>
<td>Audit the flow of information within the enterprise perimeter</td>
<td>Audit information and the WHO / WHAT / WHEN / WHERE of information</td>
</tr>
<tr>
<td><strong>What it does not do</strong></td>
<td><strong>What it does not do</strong></td>
</tr>
<tr>
<td>Enable collaboration: DLP systems actually inhibit technologies like emails &amp; USB media</td>
<td>Discover information: IRM systems do not “read through” and classify information</td>
</tr>
<tr>
<td>Control beyond perimeter: DLP systems are perimeter centric</td>
<td>Control distribution: IRM systems do not monitor or control information flow</td>
</tr>
<tr>
<td><strong>What context is it useful in</strong></td>
<td><strong>What context is it useful in</strong></td>
</tr>
<tr>
<td>Discovery: Data lying in heterogeneous systems needs to be discovered and classified</td>
<td>Security in collaborative environments: Data needs to move across perimeters and needs to be controlled</td>
</tr>
<tr>
<td>Control &amp; audit data flow: Data flow across the internal network needs to be controlled and audited</td>
<td>Granular controls: Controls beyond yes/no need to be implemented</td>
</tr>
</tbody>
</table>
The Ideal Solution

• The best of both worlds – DLP and IRM

– Content aware but can work beyond the perimeter thus managing both security and collaboration.
– Works well with content management and document management systems.
– Policies and rights are implemented on information and all its copies where ever they are transmitted or stored.
– Integration of these technologies with sources of information like core business applications so that these policies are applied as soon as information moves into private domain.
Implementation Considerations

- Both:
  - Require clarity on where information lies, how critical it is, who has access to what. More for DLP than IRM.
  - Cannot be used for information which is small in volume.

- DLP Technologies:
  - High investment. Each user requires licenses and it is annual recurring cost in most cases.
  - Constant evolution of policies required. Full time employees required to monitor DLP technologies.
  - False positives can be high. Administrative loads can be high.
  - Policy creation and management is centralized.
  - Exceptions can make system useless over a period of time.
  - Load on existing information systems.
  - Most products don’t support mobile devices yet.
  - Content search technology is evolving.
Implementation Considerations

• IRM:
  - Is not content aware and doesn’t bother about content. However some solutions integrate with DLP and provide this functionality.
  - Works on documents hence important to ensure all required file formats are supported.
  - Require a client on every system that needs to access information/documents.
  - Requires internet access at least once for rights to be downloaded.
  - Information creators are responsible for protection though rights application can be forced.
  - Some licensing models require readers / users to have licenses. It may be difficult to predict how many licenses are required up front when collaborating.
Q & A
Thank you

Ramadan Mubarak

arun@elitetechno.com