Do you feel the pain?

- No standards
- No architectures
- No money
- Many products
  - None of which work together
  - All of which make the same claims, despite conflicting features.

The Pragmatic Philosophy

- Keep it simple
- Keep it practical
- Start small
- Grow iteratively
- Eat the elephant
- Document everything
Data Breach Triangle

BASIC

Pragmatic Data Security Cycle
Advanced

The Information-Centric Security Lifecycle

Create
- Classify
- Assign Rights

Store
- Access Control
- Encryption
- Rights Management
- Content Discovery

Use
- Activity Monitoring
- and Enforcement
- Rights Management
- Logging
- Control
- Application Security

Share
- Encryption
- Asset Management

Archive
- Content Encryption

Destroy
- Secure Erasure
- Content Erasure

The Two Sides of Data

Data Center

Productivity
Getting Started

Discover

1. Define sensitive data.
2. Find it.
3. Correlate back to users.
### Techniques

<table>
<thead>
<tr>
<th>DLP</th>
<th>DAM</th>
<th>Network Tools</th>
<th>eDiscovery/Classification</th>
<th>FOSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Network monitoring - Server/endpoint discovery - Some DB discovery</td>
<td>- DB only - Not all tools support</td>
<td>- WAF/UTM - IPS/etc. - Many now include RegEx monitoring - Extremely limited</td>
<td>- Servers/storage - Limited analysis</td>
<td>- Network and storage - Basic RegEx - Some file cracking</td>
</tr>
</tbody>
</table>

### VA and Pen Testing

- Find vulnerabilities
- Focus on sensitive data stores.
- Use specialized tools for web apps and databases.
- Penetration test
- Validates risks.
- Determines information exposure.
What You Should Do

- Start with 1-3 data types.
- Use CMP/DLP to find them in storage and on endpoints.
- Use DAM/ADMP (or CMP) to find in databases.
- FOSS tools can help for basic data/PII, but not IP.

Secure

- Fix access controls.
- Remove unneeded data.
- Lock down access channels.
- (Maybe) encrypt
The Three Laws of Encryption

- If Data Moves Physically or Virtually
- For Separation of Duties
- Mandated Encryption

Where to Encrypt

Separation of Duties
- Database Fields
- Workstation
- File/Folder
- Server
- NAS
- Applications

Movement/Media Protection
- Tape
- SAN
- Laptops/FDE
- Email
- Portable Media

Encryption Options

- File/Folder
- Application/Database
- Media
Encryption Layers

Access Channels

Data Masking
Data Masking

What You Should Do

- Remove/quarantine viral data.
- If you can’t map access controls to users, just lock it down and manage exceptions.
- Encrypt laptops, backup tapes, and portable media.
- Lock down application and database access channels.
- Begin data masking.

Monitor

- DLP/CMP for the network, storage, and endpoints.
- DAM/ADMP for databases.
- Egress filtering.
- Other tools may help, but give a false sense of security.
Incident Management

<table>
<thead>
<tr>
<th>ID</th>
<th>Time</th>
<th>Policy</th>
<th>Channel/Location</th>
<th>Severity</th>
<th>User</th>
<th>Action</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1138</td>
<td>1625</td>
<td>PII</td>
<td>eMSSM/Email</td>
<td>1.2 M</td>
<td>rmogull</td>
<td>Quarantine</td>
<td>Open</td>
</tr>
<tr>
<td>1139</td>
<td>1632</td>
<td>HIPAA</td>
<td>IM</td>
<td>2</td>
<td>jsmith</td>
<td>Notified</td>
<td>Assigned</td>
</tr>
<tr>
<td>1140</td>
<td>1702</td>
<td>PII</td>
<td>Endpoint/HTTP</td>
<td>1</td>
<td></td>
<td>None</td>
<td>Closed</td>
</tr>
<tr>
<td>1141</td>
<td>1712</td>
<td>R&amp;D/Product X</td>
<td>USB</td>
<td>4</td>
<td>bgates</td>
<td>Notified</td>
<td>Assigned</td>
</tr>
<tr>
<td>1142</td>
<td>1730</td>
<td>Financials</td>
<td>dba/C$</td>
<td>4</td>
<td>sjobs</td>
<td>Quarantine</td>
<td>Escalated</td>
</tr>
</tbody>
</table>

DB Auditing vs. Activity Monitoring

- **Native Auditing**
  - Single Platform
  - Passive
  - Locally stored (default)

- **DAM**
  - Crosses platform
  - Active alerting
  - Secure repository
  - All activity capable
  - Additional features

Aggregation and Correlation

- Oracle
- SQL Server
- DB2

<table>
<thead>
<tr>
<th>Server</th>
<th>Query Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU1</td>
<td>CPU2</td>
</tr>
<tr>
<td>HE32</td>
<td>Update</td>
</tr>
</tbody>
</table>
Alternatives/Adjuncts

- SIEM
  - Many SIEM tools now include DAM support, or can pull (some of) audit logs.

- Log Management
  - Many also now include some database support

- Triggers
  - A bad option, but free and might be good enough under some circumstances

What You Should Do

- Focus network DLP/CMP on transaction areas first, since that's where the worst losses occur.
- Use DAM on priority databases, then expand.
- Other logging/monitoring can help, but is not content specific, and won't give great results.
- Monitor sensitive data on endpoints with DLP, especially portable storage transfers.

Protect

- Secure web applications.
- Validate encryption.
- Use DLP/CMP for network communications and endpoints.
- Set DAM policies for proactive alerting.
Web Application Security

- Secure SLOC
- Static Analysis
- Dynamic Analysis
- WAF
- Penetration Testing
- Vulnerability Scanning

CMP Deployment Modes

- **Passive**
  - Monitoring only

- **Bridge**
  - Block, but some data leaks

- **Proxy**
  - Full blocking
  - Often requires integration

Endpoint Options

- DLP/CMP for content-based blocking.
- Portable device control or encryption for gross protection.
- Monitor/shadow files with CMP or PDC.
Defining Process

- Version detected, appears in queue
- Handler confirms incident and severity
- Escalation

Egress Filtering

- Segregate sensitive networks/transactions paths
- Lock channels with firewall/UTM
- Filter content with DLP
- Application control/next gen firewalls
- Hide behind a VPN

What You Should Do

- WAFs offer the quickest protection for web applications.
- DLP/CMP for network monitoring and blocking.
  - You may use existing email and network tools to protect PII, but it will be more difficult to manage and offer less protection.
- PDC or DLP/CMP for endpoint data protection (on top of encryption).
Data Security on the Cheap

- Focus on as few critical data types as possible.
- Use FOSS or existing tools for discovery.
- Prioritize with VA and penetration testing.
- Leverage features in existing tools.
  - Email/web filtering
  - USB blocking
  - OS-based encryption

Your Best Options

- Start with DLP/CMP content discovery.
- Identify databases with sensitive data, and start activity monitoring (DAM).
  - Focus VA and penetration tests on these systems, especially if accessed via web applications. This is the single biggest channel for major breaches.
- Encrypt all laptops.
- Egress filter transaction networks.
- Slowly minimize use of protected data. Do you really need to let that many people access it? Can you consolidate it?

Rich Mogull
Securosis, L.L.C.
rmogull@securosis.com
http://securosis.com
AIM: securosis
Skype: rmogull
Twitter: rmogull