Security Metrics

What’s Hot and What’s Not
Outline

• Current State (4)
• What We Can Do (7)
• What PlexLogic is Doing
• Conclusions (1)
## IT S & M: 2010

**Key:**
- **H** >90%
- **M**
- **L** <5%

<table>
<thead>
<tr>
<th>Program</th>
<th>Tools</th>
<th>Features</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad Hoc</td>
<td>XLS, PPT</td>
<td>Report</td>
<td>Homegrown</td>
</tr>
<tr>
<td>Program</td>
<td>Homegrown</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Community</td>
<td>Market Reports</td>
<td>Homegrown</td>
<td>Cloud</td>
</tr>
</tbody>
</table>

**Tools:**
- Verizon
- Veracode
- OSF:DLDB
- SharePoint
- MySql
- Drupal
- Pentaho
- Cognos
- Hyperion
- XX-ISAC
- PlexLogic
- ClearPoint

**Platforms:**
- Archer
- Qualys
- ArcSight
<table>
<thead>
<tr>
<th>Security</th>
<th>Ad Hoc</th>
<th>XLS, PPT</th>
<th>Report Features</th>
<th>Home</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program</td>
<td>Home</td>
<td>Datamart</td>
<td>Metrics Platform</td>
<td></td>
</tr>
<tr>
<td>Community</td>
<td>Market Reports</td>
<td>Home</td>
<td>Cloud</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Medicine</th>
<th>Ad Hoc</th>
<th>XLS, PPT</th>
<th>Report Features</th>
<th>Home</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program</td>
<td>Home</td>
<td>Datamart</td>
<td>Analysis Platform</td>
<td></td>
</tr>
<tr>
<td>Community</td>
<td>Market Reports</td>
<td>Home</td>
<td>Cloud</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Baseball</th>
<th>Ad Hoc</th>
<th>XLS, PPT</th>
<th>Report Features</th>
<th>Home</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program</td>
<td>Home</td>
<td>Datamart</td>
<td>Analysis Platform</td>
<td></td>
</tr>
<tr>
<td>Community</td>
<td>Market Reports</td>
<td>Home</td>
<td>Cloud</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Finance</th>
<th>Ad Hoc</th>
<th>XLS, PPT</th>
<th>Report Features</th>
<th>Home</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program</td>
<td>Home</td>
<td>Datamart</td>
<td>Trading Platform</td>
<td></td>
</tr>
<tr>
<td>Community</td>
<td>Market Reports</td>
<td>Home</td>
<td>Cloud</td>
<td></td>
</tr>
</tbody>
</table>

Key: | H >90% | M | L <5% |
Killer Apps

- 1800s: Epidemiology - study of disease
- Biostatistics - theory of natural selection
- Bioinformatics - human genome proj.

- 1952: Markowitz - Portfolio Selection
- Black-Scholes option pricing (Nobel Prize)
- Algotrading: Stat arbitrage, sig fitting

- 1970s - Bill James
  - Beane (Oakland A’s)
  - Theo Epstein (Red Sox)
- Money Ball by Michael Lewis

- 1950s - Marketing analytics (Nielsen)
- 1981 - Six Sigma: 3M, Boeing, GE, Motorola
- 1990s - Web analytics
- 2000: eHarmony - On-line match making

(c) 2010 PlexLogic LLC. All rights reserved.
State of Market: 2010

Key:  

- Metrics deliver value (but proven elsewhere)
- Vendors: Over promise
- Practitioners: Unrealistic expectations
- Business Culture: Sharing data (Tragedy of the Anti-Commons)

- We can get killer apps

(c) 2010 PlexLogic LLC. All rights reserved.
How ?

INNOVATE

• Better Models
• Automation
• Early Adopters
Models

Key: \( \text{H} \geq 90\% \quad \text{M} \quad \text{L} \geq 5\% \)

- Counts, Percents, Ranks
- Leverage Visual Analytics
- Mimic IT Management
- Mimic Medicine
- Mimic Finance
- Mimic Economics
# Automation

<table>
<thead>
<tr>
<th>UseCases</th>
<th>Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad Hoc</td>
<td>XLS, PPT</td>
</tr>
<tr>
<td>Program</td>
<td>Homegrown</td>
</tr>
<tr>
<td>Community</td>
<td>Market Reports</td>
</tr>
</tbody>
</table>

- **Report Features**: Homegrown
- **Datamart**: Metrics Platform
- **Community**: Cloud

- **2003**: Sigma
- **2005**: ClearPoint
- **2008**: MetricsCenter
- **2010**: ClearPoint

(c) 2010 PlexLogic LLC. All rights reserved.
### Platform Feature Set

**Importance:** | **Provided:**
---|---
| H | M | Y | N |

<table>
<thead>
<tr>
<th>Feature</th>
<th>CPM</th>
<th>HG</th>
<th>IMHO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Dashboards</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Re-Usable Implementation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ad Hoc Investigation</td>
<td>Excel</td>
<td>Excel</td>
<td></td>
</tr>
<tr>
<td>Metrics Design Studio</td>
<td></td>
<td>Excel</td>
<td></td>
</tr>
<tr>
<td>Metrics Catalog</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Content Mgmt (RSS, Rating,...)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lifecycle/Workflow</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multi-Tenant/Community</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anonymization</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OLAP, Models, Dynamic Viz</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RDBMS, Static Rpts, Counting</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(c) 2010 PlexLogic LLC. All rights reserved.
Anonymization

Submitted

Re-Identified

Anonymized
Anonymization: - / +

- NP Hard
- Subject to attack
- Skepticism

- Used widely
- Attack defenses exist
- Exists as COTS
Public Dashboards

- Open Security Foundation
  http://www.opensecurityfoundation.org
- Verizon DBIR
- Veracode SOSS
  http://www.veracode.com
- MetricsCenter Dashboards
  http://www.metricscenter.net
Conclusions

#1: Killer apps
#2: Innovation
#3: Regulation

Adoption is slow but will spike