Lessons Learned in Security Measurement

Nadya Bartol & Brian Bates
Booz Allen Hamilton
Contents

• Overview
• Lessons Learned
• Case Studies
• Summary
Reasons Behind Security Metrics

- Information security measurement is still an unsolved problem
- Congress and CISOs are asking for security measurement to achieve and maintain compliance
- Quantifiable data is needed to support risk-based decision making and facilitate improvement of security
- Increased call for justifying investments and increasing accountability
Standards and Guidance

• NIST Special Publication SP 800-55 Rev1: Performance Measurement Guide for Information Security
• OMB FISMA Reporting Requirements and PART/PMA (Program Assessment Rating Tool/President’s Management Agenda)
• CMMi – Capability Maturity Model Integration®*
• ISO/IEC 15939 – System and Software Engineering – Measurement Process
• ISO/IEC 27001/27004 (draft): Information Security Management Measurement

* Capability Maturity Model, Capability Maturity Modeling, and CMM are registered in the U.S. Patent & Trademark Office
Best Practices For Good Metrics

- **Organizational acceptance**: Metrics and dashboards should be vetted through appropriate approval channels.
- **Based on security goals and objectives**: Policy, procedures and risk priorities should be used to derive measurable performance goals and objectives.
- **Quantifiable**: Metrics should be more quantitatively focused to increase the objectivity and validity of data.
- **Obtainable/feasible**: Metrics data should be available or easily collected through interviewing or by accessing data repositories.
- **Repeatable**: Metrics and process should be easily repeatable in a standard way at predetermined intervals to identify performance trends over time.
- **Relevant and meaningful reports**: Metrics should be displayed in the appropriate format to the appropriate stakeholder level.
- **Useful beyond measurement**: Metrics should be useful to stakeholders and should yield information that is important in the decision making process.
Relationships with Other Security Functions

Outputs from every security program function and component can be used as inputs for metrics...

...and outputs from metrics analyses can be used to improve every security program function and component.
Lessons Learned – Data Collection

• **Common pitfalls of data collection**
  – Data sources not considered or defined
  – Not collected from start or collected incorrectly
  – Deemed to difficult to collect after first cycle
  – Difficulty or inability to capture historical data

• **How to make it work**
  – Identify all available data and select what you need
  – Define data collection upfront including changes to processes or tools
  – Use feasibility of data collection as one of the criteria for metrics selection
  – Train your data collectors and information owners about what you need and then ask for it repeatedly
Lessons Learned – Long Term Focus

• **Organizations lose interest and focus in metrics rather quickly**
  – Interest is high when security is a focus
  – When all is good and in the green, metrics are an afterthought
  – Accountability for metrics not correctly assigned
  – Turnover and changes in roles breaks up continuity

• **How to make it work**
  – Obtain management commitment before you start
  – Manage expectations continuously – explain that the long term focus is critical
  – Iterate the program to measure critical things
  – Assign roles, train your responsible parties, and communicate that continuity is key for success
Lessons Learned – Using Metrics

• **Metrics data not used or displayed correctly**
  – Focus of metrics analysis and reporting not based on a prioritization schema (e.g., Risk, Compliance, ROI)
  – Wrong metrics distributed to the wrong stakeholders
  – Metrics data is not reused or used for decision making or improvement

• **How to make it work**
  – Understand why you are collecting metrics and prioritize when you set up the program
  – Define who gets what data and reassess periodically – ask your customers if it is still useful
  – If metrics are not used for decision making and improvement, drop them
  – Communicate, communicate, communicate
Success Stories – Example 1

**Organization**
Enterprise security program support that included enterprise continuous monitoring, security metrics, dashboards, and security change management

**Key Issues**
- Difficulty implementing measurement and monitoring processes consistent with security requirements and standards
- Resource intensive, untimely, and redundant collection resulting in inefficiently and inaccurate data

**Scope**
- Documentation and implementation of enterprise measurement and monitoring approaches
- Executive and operational level metrics reports and dashboards that contain near real-time status and progress
- Identification, prioritization, and mitigation of program and system weaknesses to drive process improvement

**Impacts**
- Consistent gains in compliance scores
- 100% of systems received security measurement and monitoring in FY08
- Efficient collection and reuse of metrics data
## Success Stories – Example 2

<table>
<thead>
<tr>
<th>Organization</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise security program support that included system and program level security metrics and dashboards</td>
<td>• Performance Measurement Program Implementation Plan and Standard Operating Procedures</td>
</tr>
<tr>
<td></td>
<td>• Centralization of the collection and warehousing of performance measurement data</td>
</tr>
<tr>
<td></td>
<td>• Security metrics collection, analysis, and reporting via 130+ quarterly/annual metrics across 13 workstreams</td>
</tr>
<tr>
<td></td>
<td>• Executive and operational metrics reports and dashboards</td>
</tr>
</tbody>
</table>

### Common Key Issues
- Difficulty understanding and track current status of compliance related activities
- Lack of tools and central repositories to effectively manage security measurement and monitoring data

### Impacts
- Proactive measurement of compliance goals that demonstrated continuous improvement
- Efficient reuse of centralized security metrics and data for other program efforts
- Supported substantial improvement in FISMA score
Metrics Dashboards – Example 1

This dashboard example was used to report progress and status of security metrics.

For this implementation, the SharePoint portal was leveraged.

Metrics data from eye charts can easily be pulled into collaboration sites.

Combination facilitates availability of metrics data to stakeholders using a common internal location.
Metrics Dashboards – Example 2

This dashboard example was used to report progress and status of security metrics.

For this implementation, the Plumtree portal was leveraged.

Allows organization to identify which areas require work and improves ability to properly focus and allocate resources.

Use of centralized, web-based dashboards portlets allows for easy customization of metrics graphics and sub-reports.
Metrics Dashboards – Example 3

This example was used to report security implementation, efficiency, effectiveness, and impact metrics.

A third-party COTS software was used to design, create, and implement the dashboard.

Displays metrics/key performance indicators (KPIs) on a single page or logical groupings through tabs or pages.

Rapidly transforms metrics data into meaningful, visually stunning, and interactive security information.
Summary

• Information security measurement has challenges:

• It is conceptually simple yet
  – Requires educating decision makers
  – Not glamorous and might require convincing
  – Might take a long time for organization not set up for it

• Must be done strategically and methodically

• Requires behavioral and organizational change

• To succeed you must have leadership support
Discussion