MEANINGFUL SECURITY METRICS

MEASURING COVERAGE AND CONTROL

CYNTHIA HARRIS, CISM, PMP
2 AGENDA

• What do you mean by meaningful security metrics?
• Characteristics of good metrics
• Leveraging industry frameworks and models
• Process for developing metrics
• Delivering the right metrics for your audience
• Use of visualization to understand and communicate key messages
Benefits of Meaningful Security Metrics

- Convey a clear picture (point-in-time) or historically
- Signify valuable and actionable information
- Provide support for business objectives
“security leader now need to also be a business leader and to be a business leader you have to look at your peers and leadership and all of those folks have metrics that they use every day to run and manage your business you need indicators of the health of what you're doing and so if you're running a security organization and you don't have some type of metrics package then you don't really know how effective your organization is at accomplishing its mission.”

David Komendat, VP and CSO for Boeing
5 CHARACTERISTICS OF A GOOD METRIC

• Aligned with business showing organizational goals and objectives are being met
• Actionable and predictive
• Based on a formal model
• Consistent
• Time-trackable
• Universally acceptable
• Using data that’s economical to collect
LEVERAGING INDUSTRY FRAMEWORKS

ISO 27002

NIST Cyber Security Framework

05 May 2017
# METRICS MODEL & LIFE CYCLE

## GOAL
### Conceptual Level
Measurement goals involve products, processes, and/or resources.

## QUESTION
### Operations Level
Questions try to characterize the object of measurement in the context of a qualified issue from a particular viewpoint.

## METRIC
### Quantitative Level
Associated with every question is a set of data, either subjective or objective, that helps provide quantitative answer.

<table>
<thead>
<tr>
<th>Q1</th>
<th>Q2</th>
<th>Q3</th>
<th>Q4</th>
<th>Q5</th>
</tr>
</thead>
<tbody>
<tr>
<td>M1</td>
<td>M2</td>
<td>M3</td>
<td>M4</td>
<td>M5</td>
</tr>
<tr>
<td>M6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Metric Lifecycle**

1. Identify the Right Metric (GRM)
2. Define & Classify Metric
3. Identify & Refine Data Capturing Mechanism
4. Communicate to the stakeholders
5. Capture & Validate Data
6. Analyze & Process Data
7. Report Metrics
8. Revise & Improve Metrics & Goals
8 DELIVERING THE RIGHT METRICS FOR YOUR AUDIENCE

C-SUITE & BOARD MEMBERS
- Current State of Security (Hygiene/Health)
- Current Risk Posture and Changes Over Time (trends)
- Security Initiative Performance (investments)
- Regulatory Compliance Reports / Updates Benchmark Reports
- Budget Performance

MANAGEMENT
- Trend Analysis Data
- Security Posture Trends
- Vulnerability Management / Patch Reporting
- Emerging Network Threats
- Incident Response Times
- Audit Compliance and Findings
- % of Risk Accepted Threats

SERVICE OWNERS & SUPPORT TEAMS
- # of Incidents Investigated
- Type and Severity of Security Incidents
- Vulnerability External / Internal (Highs/Mediums/Lows)
- % Servers, Apps, Patched to Current Patch Level
- Detail info on Threats
- Top/Emerging Exploits
UNDERSTAND YOUR AUDIENCE

Things to consider as you tailor your security messages for your audience

• What is the person’s area of responsibility?

• Why is the person important to information security?

• What’s valuable to this key stakeholder?

• What are their security needs?

• What information do you need from this person?
Goal Question Metric (GQM) is a simple, three step process for developing metrics

- **Purpose:** To (evaluate, predict, etc.) the (metric, process, service, etc.) in order to (understand, assess, manage, improve, etc.) it.

- **Perspective:** Examine the (costs, effectiveness, changes, etc.) from the point of view of the (manager, customer, corporate perspective, etc.)

- **Environment:** The environment consists of the following: process factors, people factors, problem factors, methods, tools, constraints, etc.
USE OF VISUALIZATION TO UNDERSTAND AND COMMUNICATE SECURITY ISSUES

Metrics may be visually represented in several ways:

- **Simple visualizations** may include a table/grid showing the metric result for the organization.

- **Graphical visualizations** may include time-series charts. To provide maximum insight, plotted values for each period may include stacked series for the differing incident classifications.

- **Complex visualizations** should be used for displaying the metric result for cross-sections.
TIPS ON HOW TO TAILOR YOUR MESSAGE TO SPECIFIC AUDIENCES

• Learn your audience and tailor your message accordingly
• Don’t “cry wolf”
• Avoid causing fear, uncertainty and doubt
• Ensure your communication are two-way rather than one-way
• Don’t say “no” to the company priority
• Deliver on your commitments

Source: Security Metric’s A Beginners Guide by Caroline Wong
WHERE TO START?

RECOMMENDATION

- Start small
- Integrate these metrics into your processes
- Grow the number of the metrics you collect
RESOURCES

1. PRAGMATIC Security Metrics: Applying Metametrics to Information Security by Brotby, W. Krag
4. Security Metrics: Replacing Fear, Uncertainty, and Doubt by Jaquith, Andrew
5. The CIS Security Metrics November 1st 2010