

C-Level Security Metrics: What Executives Want to Know and What They Don't!

Joseph W. Popinski Ph. D.

CISSP CISM, CFE, CPP

April 8, 2010



Smart Security Metrics

- What Are Smart Security Metrics?

Specific

Measurable

Attainable

Repeatable

Time-Dependent

Specific

- 1. Provide a characterization of a very narrow result or outcome**
- 2. Meet a business goal or objective**
- 3. Used in the decision making process.**

Some examples:

Numeric sales for the Month - \$000

Percent project complete this week - 48%

Daily production of widgets - 6,400 units

Measurable

1. **Easily quantified or calculated**
2. **Information/data source available**

Some examples:

Sales for the Month – aggregated from individual sub-unit sales report (numeric)

Percent Project Complete – calculated from a project status report or project control system

Daily Production of Widgets - obtainable from production control systems

Attainable

1. **Can be obtained from existing data, processes, and/or programs**
2. **Do not require extraordinary compilation effort**

Examples:

Monthly Sales as % of Goal

Average Daily Production vs. Capacity

Repeatable

1. **Recurring each reporting period**
2. **Once determined, can be duplicated**

Examples:

Monthly Sales for Past 12 Months

Average Daily Production vs. Capacity for Month

Time-Dependent

1. **Recurring each reporting period**
2. **Once determined, can be duplicated**

Examples:

Monthly Sales

Weekly Project Completion Percentage

Daily Production

Useful Metrics

- Indicate the degree to which security goals are being achieved
- Drive actions to improve security programs
- Focuses on executive management interests

Value of Security Metrics

- **Effective Tool to Determine...**

- Effectiveness of security program components
- Identify risk levels relative to actions
- Assist in prioritizing corrective actions

- **Answers...**

- Are we more secure today than we were before?
- How do we compare to others in this regard?
- Are we secure enough?

A Security Metrics Program in 8 Steps

1. Understand the underlying corporate framework

- “Six Sigma Strategy” to eliminate defects (vulnerabilities)
- corporate security standards compliance (how close)
- audit-based to verify compliance with industry standards

2. Define metrics program goals and objectives

- Goal(s) and objectives must be well-defined and agreed upon up front
- e.g. “Provide metrics that clearly and simply communicate how efficiently and effectively our company is balancing security risks and preventive measures, so that investments in our security program can be appropriately sized and targeted to meet our overall security objectives.

A Security Metrics Program in 8 Steps

3. Decide which metrics to generate

Top Down	
a. Define/list objectives of the overall security program	Example objective: To reduce the number of virus infections within the company by 30% in the next 12 months
b. Identify metrics that would indicate progress toward each objective	Example metric: Current ratio of virus alerts to actual infections as compared to the baseline year figure
c. Determine measurements needed for each metric	Example measurement: Number of virus alerts issued to the organization by month Example measurement: Number of virus infections reported

A Security Metrics Program in 8 Steps

4. Develop generation strategies

- Source of the data
- Frequency of data collection
- Who is responsible for raw data
- Accuracy
- Data compilation (measurements)
- Generation of the metric

5. Establish benchmarks and targets

- “Best Practices”
- OWASP (web apps)
- CIO Magazine

A Security Metrics Program in 8 Steps

6. Determine how to report metrics

- Over-simplification is a mistake
- Complex security-related data can be valuable to financial executives (if presented well)
- Graphic representations are particularly effective

7. Create an action plan

- Must contain all tasks to implement security metrics program
- Must include expected completion dates and assignments
- Directly derivable from objectives

8. Establish formal review/refinement program

- Regular reexamination of the entire security metrics program
- Continuous monitoring to fine-tune the program

You Must Automate the Process

- **Eliminate “Mouse Pushing”**
 - **Typical Weekly PowerPoint Dashboard (2-3 slides)**
 - ◆ Takes ~ 16-24 hours = 6/10 of a MAN-YEAR
 - ◆ At \$ 175/hr (loaded) this is \$ 218,400
 - ◆ Can you afford this for 3 charts?
- **Service Oriented Architecture**
 - **Extract data: real or near-time (on-demand or short intervals)**
 - **Appropriate amalgamation/derivation of information**
 - **Presentation in concert with BUSINESS GOALS**
- **Let Computers Do All the Work**
 - **Based on Business Requirements**
 - **Support Decision Making by C-Levels**
 - **“Less is More” Approach**

Metric Evaluation Tenants

1. **Display Honors Boundary of Single Screen**
2. **Supply Adequate Context for Data**
3. **Display in Appropriate Detail**
4. **Choosing an Appropriate Measurements**
5. **Choosing an Appropriate Display Media**
6. **Avoid Meaningless Variety**
7. **Use Effective Display Media**
8. **Encoding Quantitative Data Accurately**
9. **Effective Arrangement of Data**
10. **Important Data is Highlighted**
11. **Avoid Use of Useless Decoration**
12. **Appropriate Use of Color**
13. **Attractive Visual Display**

Examples

All Computers

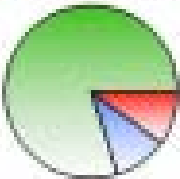
McAfee SECURITY McAfee Protection Manager

General Policies Scheduled Tasks

Manage All Computers

Compliance

View summary information for all computers



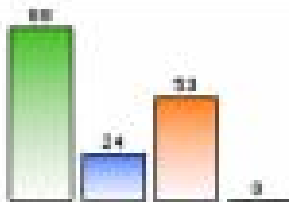
Updated	16	60%
Pending	2	10%
Not communicating	0	0%
Not up-to-date	2	10%
Total	30	

View summary information for all groups

Detection

View summary information for all computers

Last 30 days

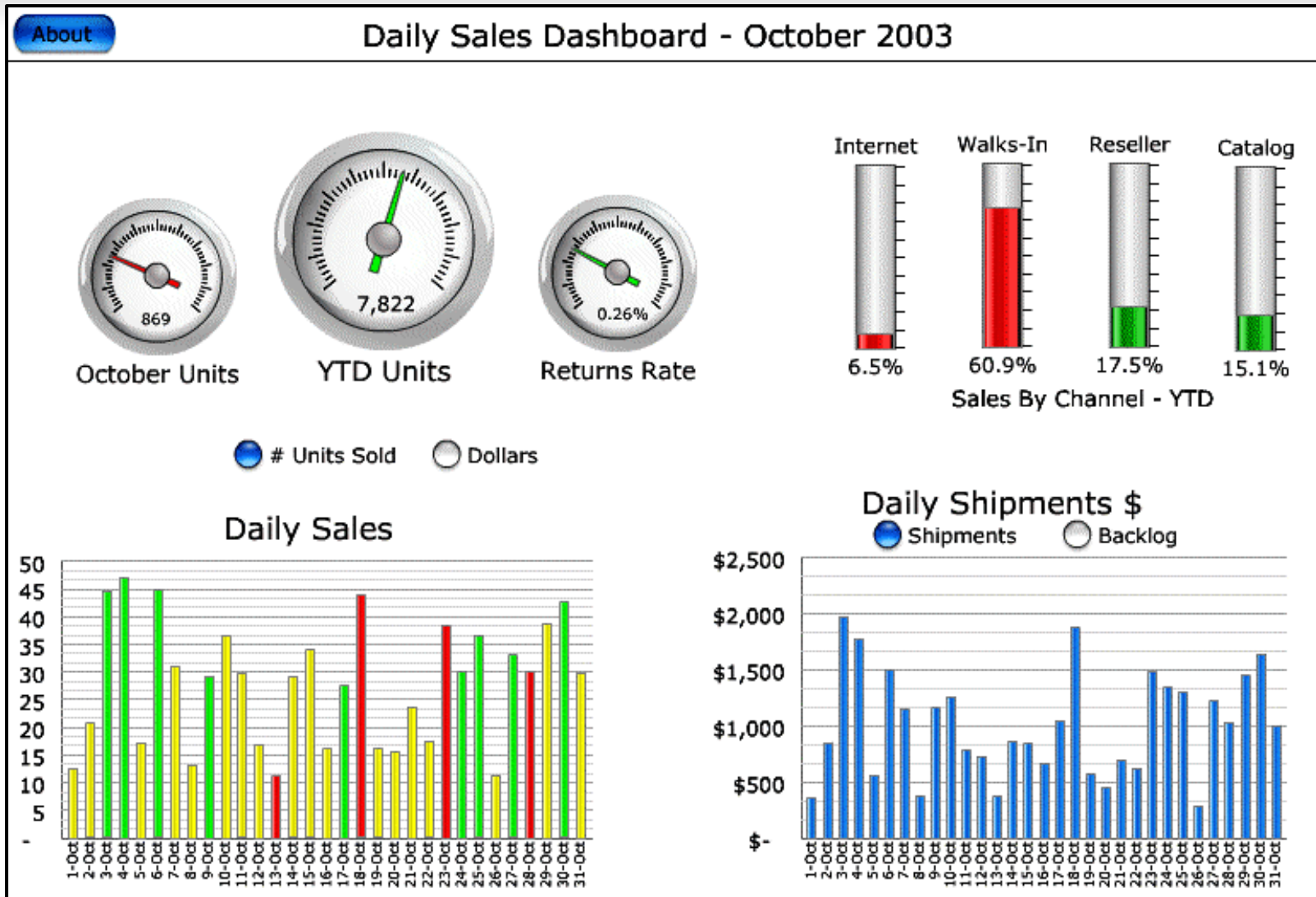


Cleaned / Masked	88	63%
Deleted	24	17%
Quarantined	53	38%
Error	0	0%
Total	165	

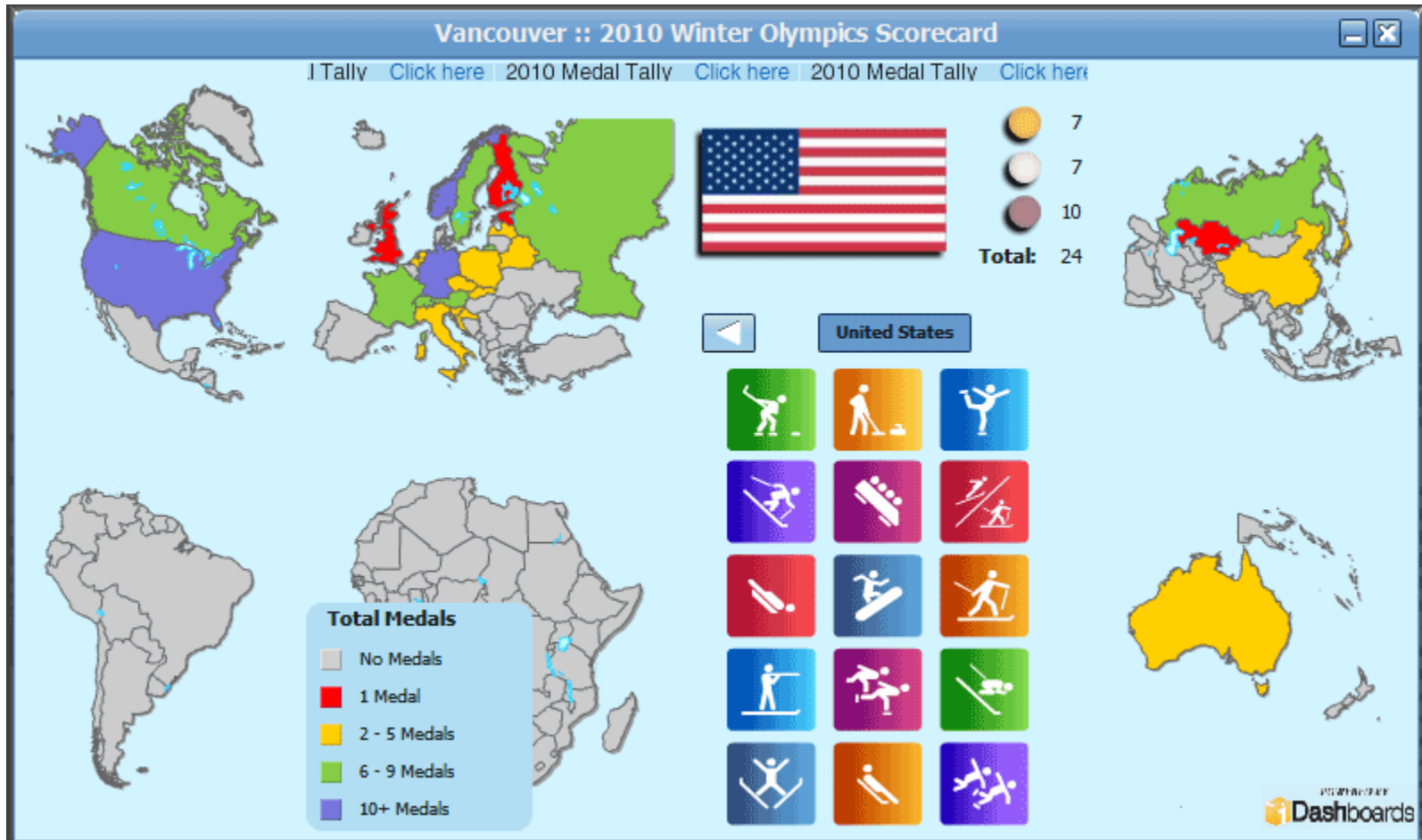
Management Tools

- Add Group
- Add Computers
- Deploy
- Refresh
- Scan
- Enforce
- Refresh

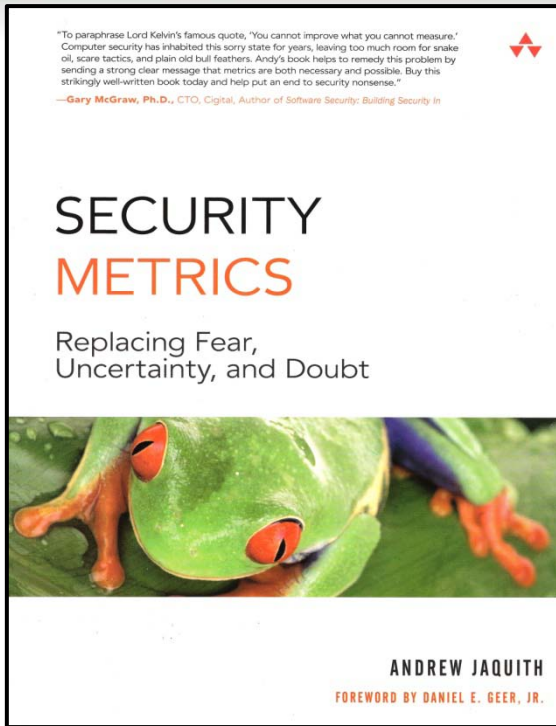
Examples



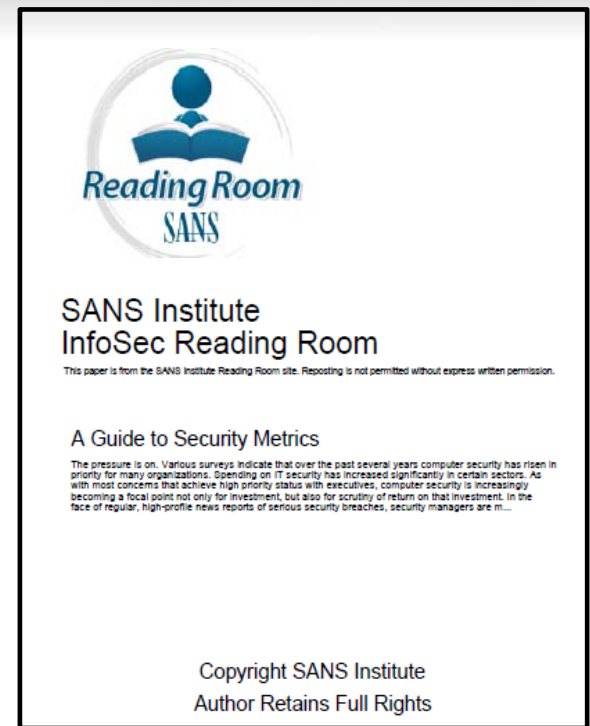
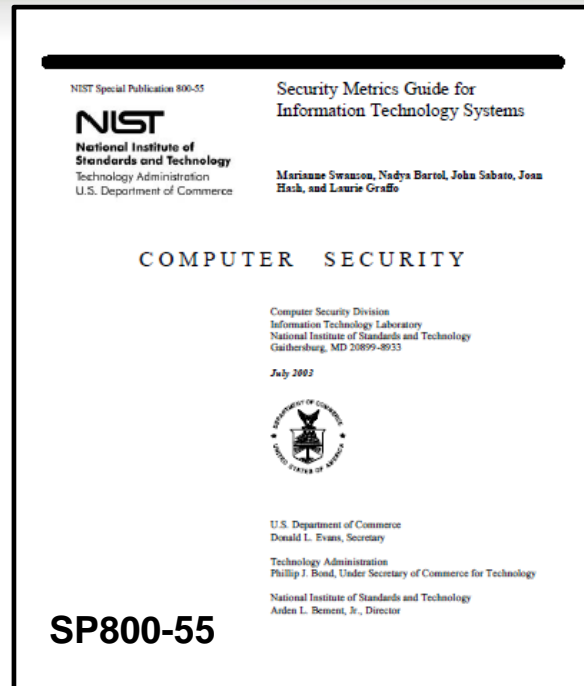
Examples



References



Author of Lophcrack



SANS Sec-410



www.simplecomplexity.net

Summary

- **Be SMART**
 - **Specific, Measurable, Attainable, Repeatable & Time-Dependent**
- **Drive Actions & Focus on Executive Interests**
- **8-Step Process to Build Good Metrics**
- **Must Automate Process**
 - **Don't Be A Mouse-Pusher**
- **Evaluation Tenants (14)**
- **Examples**

Questions ?