Collecting and Sharing Security Metrics – the End of “Security by Obscurity”

a.k.a Communicating Security Performance to Non-Security Professionals

Jim Acquaviva
nCircle

Session ID: SPO2-204
Session Classification: Intermediate
The Quarterly Ritual
## The Quarterly Ritual

### Company Financials

<table>
<thead>
<tr>
<th>Quarter Ending</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
<th>Trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>Year</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>January 2011</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>March 2011</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>June 2011</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>September 2011</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>December 2011</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### EBITDA

<table>
<thead>
<tr>
<th>Item</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cash</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Net Income

<table>
<thead>
<tr>
<th>Item</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
</tr>
</thead>
<tbody>
<tr>
<td>Earnings Per Share</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Current Liabilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Gross Margins

<table>
<thead>
<tr>
<th>Item</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Income</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Current Assets</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Current Assets

<table>
<thead>
<tr>
<th>Item</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Liabilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cash</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Current Liabilities

<table>
<thead>
<tr>
<th>Item</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cash</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Cash Flow

<table>
<thead>
<tr>
<th>Item</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cash</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Current Assets

<table>
<thead>
<tr>
<th>Item</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cash</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Current Liabilities

<table>
<thead>
<tr>
<th>Item</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cash</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Cash Flow

<table>
<thead>
<tr>
<th>Item</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cash</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The CSO needs what the CFO has....

- CISO’s need metrics language to describe a company’s security performance just like the CFO describes financial performance
  - Objective, fact-based reporting
  - Consistent definitions
  - Measured on a repeating schedule to show trends
  - Demonstrated performance against goals
  - And performance against peers
With a Security Performance Management Program, CISOs can demonstrate that

- There is a comprehensive approach to security that is…
  - Measured against specific goals & standards
  - In line with our risk tolerance
  - Aggregated by meaningful asset groupings
  - At least equal to or better than our own industry's investment & performance
  - Controls aligned with GRC objectives

- Based on actual data on an ongoing basis that we can rely on to make decisions on:
  - Investment
  - Execution
  - Resource allocation
Measuring Security is a Top CISO Priority but it is Challenging

- Heterogeneous and dispersed silo’s of vital IT information
- Variety of contributors and application sources each doing it differently
- Need to fuse together silo’s and map results to a business context
- Challenging to reliably and consistently calculate
-Exacting to communicate effectively to wide variety of audiences
Well Constructed Security Metrics & Scorecards

- Align security initiatives with business objectives
- Deliver trusted, timely, and actionable decision making information
- Identify and communicate concentration of risks
- Affirm the existence and effectiveness of security controls
- Continuously monitor controls
- Enable and evidence management oversight; communicate performance and evaluate corrective actions
Valuable Peer Benchmarks

Average Virus Definition Age
How frequently are virus definitions updated? How does this compare to the Benchmark community?

Purpose
This Benchmark Comparison Scorecard charts our average virus definition age compared to nCircle benchmark results.

We are in the First Quartile
- Quartile 1: 25
- Quartile 2: 33
- Quartile 3: 40

Analysis
Bars at or below the line indicate that our average virus definition age is within benchmark norms. This information can be used to determine whether virus definitions are updated according to policy and determine if adjustments to policy should be made.

Further Analysis
Examine the impact our average virus definition age has on detecting virus events. See the Virus Remediation Activity Scorecard, available in the Basic Endpoint Protection Benchmark Metrics Pack.

Benchmark Performance Quadrants
Participant Results
Weekly Performance Benchmark
Benchmark Performance Standard
Communicate Security and Compliance Posture: Metrics & Scorecards Roll-ups and Drill-in’s

Overview by Initiatives and by Divisions

Initiative Scorecards Across Divisions

Overviews of Initiatives and Profiles of Users and Assets are rolled-up to the executive level

Metric results are weighted and aggregated to provide control, policy, and initiative key indicators

Initiative and Security Process Scorecards

Control metrics are composed of metric results compared to policies and goals

Detailed Operational Security Metrics and Scorecards
Methodology

- Align operational tasks with strategic goals
- Drive performance organization-wide
- Based on hard facts and data
Attributes of an Actionable Metrics and Scorecards

- Controls aligned with GRC objectives
- Assigned ownership
- Measured against specific goals & standards
- Benchmarked against peer performance
- Aggregated by meaningful asset groupings
- Visuals targeted at audience
Initiative Roll Up
Example - Identity & Access Management

Protect Identities

- User Access
  - Access Removal
    - Account Deprovision Exposure
    - Account Deprovision Ticket Performance
  - Access Control
    - Account Provision Exposure
    - Account Provision Ticket Performance
  - Support Activity
    - Account Change Exposure
    - Account Change Ticket Performance
- User Activity
  - Logins
    - Successful Logins
    - Failed Logins
  - Support Activity
    - Login Age
  - Accounts
    - Active Accounts
    - Idle Accounts
    - Perpetual Accounts
  - Password Age
    - Password Age vs. Policy
    - Password Expiration Time
    - Password Expiration Policy
    - Accounts without Passwords
- User Authentication
  - Password Hygiene
    - Un-cracked Passwords

nCircle

12
Score Calculation Overview

Identity and Access Management
- User Access
  - Score: 95
  - Weight: 4
  - Formula: (1*0.83+5*0.95)/(1+5)
  - Score: 93
- User Activity
  - Score: 30
  - Weight: 1
  - Formula: (4*0.95+1*0.30+4*0.90)/(4+1+4)
  - Score: 70
- User Authentication
  - Score: 105
  - Weight: 1
  - Formula: (1*0.70+1*1.05+2*0.93)/(1+1+2)
  - Score: 90
  - Weight: 4

Password Hygiene
- Count (Un-cracked Passwords): 7500
- Total (Passwords): 10000
- Percentage: 75%
- Goal: 90%
- Formula: 0.75/0.90
- Score: 83
- Weight: 1

Accounts
- Count (Accounts with Passwords): 10000
- Total (Accounts): 10526
- Percentage: 95%
- Goal: 100%
- Formula: 0.95/1.00
- Score: 95
- Weight: 5
IT Security Governance Program
Example Screenshots

Section 1: Enterprise Rollup Scorecards

Section 2: Internal Benchmark Scorecards, by Asset Group
Section 1: Governance Objectives & Initiatives

- Protect the Organization
  - Protect the Infrastructure
  - Protect Information
  - Protect Identities
Organizational Overview

Scorecard Design and Navigation reflect Governance Program

Protect our Organization

Protect the
Infrastructure

Protect
Information

Protect Identities

Predict our Organization

Initiative: Protect our Infrastructure

Initiative: Protect our Identity

Initiative: Protect our Information

©2011 nCircle. This nCircle benchmark and the information contained therein, is owned solely and exclusively by nCircle. Any display, publication, transmission, transfer, distribution, provision of access to or other dissemination to a third party, in whole or in part, is strictly prohibited without nCircle’s express prior written approval.
Control Objectives - Protect the Infrastructure

- Protect the Organization
  - Protect the Infrastructure
  - Protect Information
  - Protect Identities
- Vulnerability Management
- Patch Management
- Antivirus & Endpoint Protection
- Configuration Management
Control Objectives

Protect our Information Performance Summary

Protect our Information is comprised of a series of controls:

<table>
<thead>
<tr>
<th>Control Objective</th>
<th>Trend</th>
<th>Current Score</th>
<th>Average Score</th>
<th>Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect our Infrastructure</td>
<td></td>
<td>85</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Antivirus and Endpoint Protection</td>
<td></td>
<td>94</td>
<td>93.0</td>
<td></td>
</tr>
<tr>
<td>Configuration Auditing</td>
<td></td>
<td>92</td>
<td>92.0</td>
<td></td>
</tr>
<tr>
<td>Patch Management</td>
<td></td>
<td>93</td>
<td>72.0</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Management</td>
<td></td>
<td>66</td>
<td>77.0</td>
<td></td>
</tr>
</tbody>
</table>

Each row in the table above shows the performance for each of the control objectives:

- Control Objective: Name of the control objective. Link to the Control Objective Performance Summary.
- Trend: Performance score for the prior 6-weeks. Performance score is the average of the control’s performance score.
- Current score: Current performance score.
- Average score: Average of the 6-week performance score.
- Goal: Performance relative to goal.

Scorecards

- Protect our Organization
  - Initiative: Protect our Infrastructure
    - Antivirus and Endpoint Protection
    - Configuration Management
  - Vulnerability Management
  - Patch Management
- Initiative: Protect our Identity
- Initiative: Protect our Information

Drilling in to Quickly Identify Problem areas
Controls

Drill in to detail to determine root cause

Vulnerability Management Performance Summary

Vulnerability Management is comprised of several controls:

<table>
<thead>
<tr>
<th>Controls</th>
<th>Trend</th>
<th>Current Score</th>
<th>Average Score</th>
<th>Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Management</td>
<td></td>
<td>66</td>
<td>73</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Risk</td>
<td></td>
<td>48</td>
<td>74.0</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Scan Policy</td>
<td></td>
<td>84</td>
<td>70.0</td>
<td></td>
</tr>
</tbody>
</table>

Scorecards

Protect our Organization
- Initiative: Protect our Infrastructure
  - Antivirus and Endpoint Protection
  - Configuration Management
  - Vulnerability Management
    - Vulnerability Risk
    - Vulnerability Scan Policy
  - Patch Management
  - Initiative: Protect our Identity
  - Initiative: Protect our Information
Key Performance Indicators

- Protect the Organization
  - Protect the Infrastructure
    - Vulnerability Management
    - Patch Management
    - Antivirus & Endpoint Protection
    - Configuration Management
  - Protect Information
  - Protect Identities

- Average Risk Score per Host
  - Pct Systems Severe Vulns
Key Performance Indicators

Vulnerability Risk Performance Summary

Vulnerability Risk is comprised of several key performance indicators:

<table>
<thead>
<tr>
<th>Key Performance Indicators</th>
<th>Trend</th>
<th>Current Score</th>
<th>Average Score</th>
<th>Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Risk</td>
<td></td>
<td>48</td>
<td>74</td>
<td>Red</td>
</tr>
<tr>
<td>Average Risk Score per Host</td>
<td></td>
<td>21</td>
<td>47.0</td>
<td>Red</td>
</tr>
<tr>
<td>Percent of Systems with Severe Vulnerabilities</td>
<td></td>
<td>75</td>
<td>83.0</td>
<td>Yellow</td>
</tr>
</tbody>
</table>

Each row in the table above shows the performance for each of the key performance indicators that comprise the control:
- **Vulnerability Risk**: Name and link to key performance indicator.
- **Trend**: Performance score for the prior 6-weeks. Performance score is the average of the key performance indicator's performance score.
- **Current score**: Current performance score.
- **Average score**: Average of the 6-week performance score.
- **Goal**: Performance relative to goal.

©2011 nCircle. This nCircle Benchmark and the information contained therein, is owned solely and exclusively by nCircle Technologies. Any reproduction, publication, transmission, transfer, distribution, provision of access to or other dissemination in whole or in part, is strictly prohibited without nCircle's express prior written approval.

Map Individual Metrics to KPIs
Performance Analysis

Use Benchmarks to set internal goals and baselines

Score performance based on goals & drive visual indicators

Analyze trends and build correlations between Benchmarks to establish KPI’s
Example Organization

- Cambridge Transportation Company
- ‘Green’ transportation company with the following structure:

  - Divisions: (Bicycles, Tricycles, Scooters, Wagons, Carriages)
  - Locations: (San Francisco, Boston, Atlanta, London, Toronto)
  - Frameworks: (SOX)
  - Risk: (Sensitive, Non-Sensitive Assets)

- Each section will internally benchmark specific areas:
  - Divisions: (Bicycles, Tricycles, Scooters, Wagons, Carriages)
  - Locations: (San Francisco, Boston, Atlanta, London, Toronto)
  - Frameworks: (SOX)
  - Risk: (Sensitive, Non-Sensitive Assets)
Scorecards provide results across security product/domain

Scorecards for each organizational view, can by managed by ACL
Contextual Scorecards (By Location, By Division)

Internally Benchmark by comparing asset groups

Standardized metrics and scorecards across asset classes.
Lessons Learned - Attributes of Successful Security Metric Initiatives

- Aligned with the organizations governance objectives & organizations strategy
- Measured against specific goals & standards
- Metrics are derived from real facts and data obtained from the enterprise.