You Can’t Manage What You Don’t Measure
Applying the Four Disciplines of Execution to an Information Security Program

Thomas Eck
Director
Security Programs & Strategy
Thanks
It is wrong to suppose that if you can’t measure it, you can’t manage it – a costly myth.

-Deming

If you can’t measure it, you can’t improve it

-Drucker
Case Study

• Fortune 250 Company

• Internal Audit finding to leverage quantitative measurement of the organization’s security program

• EVP’s “Book Club” Reading Assignment
The Measurement Challenge
Maturity Level 5: Optimizing

Stable and flexible. Organization is focused on continuous improvement and is built to pivot and respond to opportunity and change. The organization’s stability provides a platform for agility and innovation.

Maturity Level 4: Quantitatively Managed

Measured and controlled. Organization is data-driven with quantitative performance improvement objectives that are predictable and align to meet the needs of internal and external stakeholders.

Maturity Level 3: Defined

Proactive, rather than reactive. Organization-wide standards provide guidance across projects, programs and portfolios.

Maturity Level 2: Managed

Managed on the project level. Projects are planned, performed, measured, and controlled.

Maturity Level 1: Initial

Unpredictable and reactive. Work gets completed but is often delayed and over budget.
BUT...
ONE SIZE DOES NOT FIT ALL
A Challenging Paradox…

COMMUNICATION

Expert Knowledge

Ability to Demand Action of Others
POINTS
100
WHEN LIT
The Curse of Knowledge
Typical Scorecard Issues: A Summary

- Too much of the wrong data presented to the wrong audience
- We shouldn’t assume knowledge or ability to interpret data correctly
- Fail to use concrete language that naturally leads to the actions you want taken
CONSULTANTS.

ENOUGH SAID.
BUT WAIT

THERE'S MORE
(Another) Masterpiece Opportunity
ACTIONABLE
RELEVANT
CONCRETE
DYNAMIC
4DX = The 4 Disciplines of Execution

CHRIS McCHESNEY
SEAN COVEY
JIM HULING

ACHIEVING YOUR WILDLY IMPORTANT GOALS

#1 Business Bestseller
The Wall Street Journal

FOREWORD BY CLAYTON CHRISTENSEN
4DX Recap: 352 Pages in Four Bullets

• Choose one or two (but no more) **Wildly Important Goals** in the form of “change X to Y by this date”

• Choose your **Lead Measures** in the form of simple, measurable actions you can do each day that will help you reach your goals

• Keep a compelling **Scoreboard** which tells you at a glance whether you’re on target to hit your goals or not

• Hold regular **accountability sessions** to review the scoreboard and discuss progress
Lead Metrics versus Lag Metrics

Current Weight

vs.

Calories In – Calories Expended
Focus on What is Wildly Important

• Create a universe of possible metrics, but present only those that support the story you need to tell

• If you have to present everything, create an appendix or use an executive summary to avoid “burying the lede”

• Communicate what is necessary to keep people accountable
YOU'RE WELCOME
The CASE Method: An Effective Methodology

Copy and Steal Everything
CIS Consensus-based Metrics

• Derived based on consensus of 150 industry experts

• Detailed definitions of 28 metrics across 7 different functions:
  o Incident Management
  o Vulnerability Management
  o Patch Management
  o Application Security
  o Configuration Management
  o Change Management
  o Financial Metrics
CIS Consensus-based Metrics

• Each CIS metric definition provides the following:

  - Metric Name
  - Description
  - Type
    - Management
    - Operational
    - Technical
  - Audience
    - Business Management
    - Security Management
    - Security Operations
    - Operations
  - Question
  - Answer
  - Formula
  - Units
  - Frequency
  - Targets
  - Potential Data Sources
  - Visualization Recommendations
## CIS Consensus-based Metrics

<table>
<thead>
<tr>
<th>Function</th>
<th>Management Perspective</th>
<th>Defined Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Management</td>
<td>How well do we detect, accurately identify, handle, and recover from security incidents?</td>
<td>• Cost of Incidents&lt;br&gt;• Mean Cost of Incidents&lt;br&gt;• Mean Incident Recovery Cost&lt;br&gt;• Mean-Time to Incident Discovery&lt;br&gt;• Number of Incidents&lt;br&gt;• Mean-Time Between Security Incidents&lt;br&gt;• Mean-Time to Incident Recovery</td>
</tr>
<tr>
<td>Vulnerability Management</td>
<td>How well do we manage the exposure of the organization to vulnerabilities by identifying and mitigating known vulnerabilities?</td>
<td>• Vulnerability Scanning Coverage&lt;br&gt;• Percent of Systems with No Known Severe Vulnerabilities&lt;br&gt;• Mean-Time to Mitigate Vulnerabilities&lt;br&gt;• Number of Known Vulnerability Instances&lt;br&gt;• Mean Cost to Mitigate Vulnerabilities</td>
</tr>
</tbody>
</table>
## CIS Consensus-based Metrics

<table>
<thead>
<tr>
<th>Function</th>
<th>Management Perspective</th>
<th>Defined Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patch Management</td>
<td>How well are we able to maintain the patch state of our systems?</td>
<td>• Patch Policy Compliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Patch Management Coverage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Mean-Time to Patch</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Mean Cost to Patch</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>What is the configuration state of systems in the organization?</td>
<td>• Percentage of Configuration Compliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configuration Management Coverage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Current Anti-Malware Compliance</td>
</tr>
<tr>
<td>Change Management</td>
<td>How do changes to system configurations affect the security of the organization?</td>
<td>• Mean-Time to Complete Changes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Percent of Changes with Security Reviews</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Percent of Changes with Security Exceptions</td>
</tr>
</tbody>
</table>
## CIS Consensus-based Metrics

<table>
<thead>
<tr>
<th>Function</th>
<th>Management Perspective</th>
<th>Defined Metrics</th>
</tr>
</thead>
</table>
| Application Security | Can we rely on the security model of business applications to operate as intended?     | • Number of Applications  
• Percent of Critical Applications  
• Risk Assessment Coverage  
• Security Testing Coverage |
| Financial Metrics | What is the level and purpose of spending on information security?                     | • IT Security Spending as % of IT Budget  
• IT Security Budget Allocation |
Data Sources

• Vulnerability scan data
• Policy enforcement data
• DLP and incident tracking tool data
• Phishing campaign results
• Reconciliation across disparate data sets
  o HR and Active Directory (Users)
  o HR and Phishing Campaign Data (Users)
  o Active Directory and Antivirus Database (Clients)
  o Active Directory and Vulnerability Scanning inventory (Clients and Networks)
Differing Audiences: The Metrics Hierarchy

• We want to focus on building *lead measures at the Operational level*

• We also want to build a *hierarchy of metrics* that directly show the relationship between metrics needed to support each audience
Applying the Key Concepts
<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Description and Associated Risk</th>
<th>Metric Value</th>
<th>Target Value</th>
<th>Status</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ability to Enforce Server Standards</td>
<td>Non-compliant devices are not aligned with established security standards enforced by Qualys. This metric measures the number of servers that are reporting health Qualys client installations.</td>
<td>97%</td>
<td>&gt;95%</td>
<td>OK</td>
<td>Review list of missing devices; identify root cause and take corrective action</td>
</tr>
<tr>
<td>Alignment with Wintel Server Standards</td>
<td>Non-compliant devices are not aligned with established security standards enforced by Qualys. This metric measures the percentage of devices with a “passing” compliance score within Qualys.</td>
<td>82%</td>
<td>90%</td>
<td>Investigate</td>
<td>Continue efforts to remediate non-compliant devices</td>
</tr>
<tr>
<td>Alignment with Unix Server Standards</td>
<td>Non-compliant devices are not aligned with established security standards enforced by Qualys. This metric measures the percentage of devices with a “passing” compliance score within Qualys.</td>
<td>87%</td>
<td>90%</td>
<td>Investigate</td>
<td>Continue efforts to remediate non-compliant devices</td>
</tr>
<tr>
<td>Alignment with VMWare Server Standards</td>
<td>Non-compliant devices are not aligned with established security standards enforced by Qualys. This metric measures the percentage of devices with a “passing” compliance score within Qualys.</td>
<td>98%</td>
<td>90%</td>
<td>OK</td>
<td>No action required at this time</td>
</tr>
<tr>
<td>Alignment with Network Device Standards</td>
<td>Non-compliant devices are not aligned with established security standards enforced by Qualys. This metric measures the percentage of devices with a “passing” compliance score within Qualys.</td>
<td>95%</td>
<td>90%</td>
<td>OK</td>
<td>No action required at this time</td>
</tr>
<tr>
<td>Alignment with Database Standards</td>
<td>Non-compliant devices are not aligned with established security standards enforced by Qualys. This metric measures the percentage of devices with a “passing” compliance score within Qualys.</td>
<td>65%</td>
<td>90%</td>
<td>Action Required</td>
<td>Continue efforts to remediate non-compliant devices</td>
</tr>
<tr>
<td>Metric</td>
<td>Risk Associated with Metric</td>
<td>Metric Value</td>
<td>Target Value</td>
<td>Status</td>
<td>Recommended Action</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
<td>--------------</td>
<td>--------------</td>
<td>-----------------</td>
<td>------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Aged Machine Accounts</td>
<td>Aged machine accounts may indicate broken or missing business processes associated with removing devices from the environment</td>
<td>12%</td>
<td>&lt;10%</td>
<td>Action Required</td>
<td>Trending positively. Continue investigating to remove aged machine accounts in Active Directory</td>
</tr>
<tr>
<td>Server Antivirus Coverage</td>
<td>All devices within the environment should maintain an up-to-date antivirus client installation to reduce malware-related threats</td>
<td>99%</td>
<td>&gt;95%</td>
<td>OK</td>
<td>No action required at this time</td>
</tr>
<tr>
<td>Use of Privileged Access Management Tools</td>
<td>We maintain a privileged access management tool to control, manage and track the proper use of administrative rights</td>
<td>83%</td>
<td>&gt;75%</td>
<td>OK</td>
<td>No action required at this time</td>
</tr>
<tr>
<td>Desktop Management Coverage</td>
<td>All desktops within the environment should have a valid desktop management client to facilitate patching, inventory and remote access</td>
<td>99%</td>
<td>&gt;95%</td>
<td>OK</td>
<td>No action required at this time</td>
</tr>
<tr>
<td>Desktop Antivirus Coverage</td>
<td>All devices within the environment should maintain an up-to-date antivirus client installation to reduce malware-related threats</td>
<td>94%</td>
<td>&gt;95%</td>
<td>Investigate</td>
<td>Trending negatively by ~1% – investigate why fewer devices are checking in over last month</td>
</tr>
<tr>
<td>Mobile Device Encryption</td>
<td>Non-compliant machines are not known to be running whole disk encryption and represent a potential data loss risk if the device is lost or stolen</td>
<td>95%</td>
<td>&gt;95%</td>
<td>OK</td>
<td>No action required at this time</td>
</tr>
</tbody>
</table>
- Total Machine Accounts in Active Directory: 11,161
- Windows Devices in Active Directory: 10,953
- Devices with check-in within the last six months: 8,918

Machine Account Aging:
- 0-6 Months: 81%
- 6-12 Months: 14%
- 12-60 Months: 534,5%
- 60+ Months: 13,0%
Implementing a Metrics Program

• Agreed upon relevant metrics to be collected, definitions, initial Wildly Important Goal

• Identified data sources for metrics supporting WIG
  o Derived new data through reconciliation
  o Fully automated data collection

• Reviewed specific metric performance to establish realistic targets

• Agreed format for operational and leadership scorecards
  o Data trending and Board-level scorecard replacement planned for future phase

• Socialized with stakeholders outside of Security
Summary

• Actionable, lead measures arranged hierarchically and tailored to tell the right story to each audience

• Only choose metrics from your inventory that support your Wildly Important Goal(s) and highlight the actions requested of stakeholders
  o Use the CASE Method: leverage the CIS definitions where possible
  o Reconcile across data sets for new insights

• Eliminate the need for expert knowledge in order to interpret the data by explicitly stating the actions you want taken
THANK YOU
Questions & Answers