Measuring Metrics Programs
Why Aren’t We?

Jared Pfost
jared@thirddefense.com
Blog: thirddefense.wordpress.com
The Chase

• Measuring metric program maturity would be easy, but not valuable
• Metric programs aren’t a priority for enough CISO’s for a benchmark to matter
• Additional Proof Needed: correlate metrics maturity and losses
We Can But Should We?

• Maturity of Metric Program Survey
  – Perceived Benefit of metrics
    • Communication, Measure Posture, Loss reduction
  – Perceived Cost
    • Dollars, Difficulty, Duration
  – Types of metrics used
    • Access
    • Application
    • Device
    • Network
    • Incidents
    • Policy Exceptions
    • Project Management
  – Maturity of metric program
    • CMMI scale
Will a Benchmark Make a Difference?

• Metrics don’t matter to enough people

• Results wouldn’t inspire action
  – E.g. 76% of enterprises have Ad Hoc metrics programs... (just made that up)

• We eventually need benchmarking
  – Communicate security posture
  – Key attribute of effective controls
  – Visibility helps hold control owners accountable
Let’s Get It Going

Why don’t metrics matter?

Too Hard

Solution:
• Get Vendors to improve metric reports e.g. Devices “Managed for Security” shouldn’t be so hard

Solution:
• More showcases
• Add to PCI and Regs??
• Focus on IT, not just Security e.g. CMDB

No Perceived Value

Solution:
• More evidence
Metrics reduce loss

Void of IT Leadership
Action

• Reactive: Anytime a loss occurs, measure metric maturity
  – Hypothesis: Metric Maturity is relevant to Root Cause
  – Attention breach surveyors

• Proactive:
  – ITPI type measurements
    • Determine if mature metrics programs are attributes of top performers
  – For the Believers: Require Metrics to be defined before budget approval

• Examples
  – Tripwire Cost of Compliance?
Tripwire: Cost of Compliance

Table 4: Security effectiveness attributes with the highest negative correlation to non-compliance cost

<table>
<thead>
<tr>
<th>Security effectiveness scoring attributions</th>
<th>Correlation*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor and strictly enforce security policies</td>
<td>-0.34</td>
</tr>
<tr>
<td>Conduct audits or assessments on an ongoing basis</td>
<td>-0.32</td>
</tr>
<tr>
<td>Attract and retain professional security personnel</td>
<td>-0.31</td>
</tr>
<tr>
<td>Ensure minimal downtime or disruptions to systems resulting from security issues</td>
<td>-0.30</td>
</tr>
<tr>
<td>Prevent or curtail viruses, malware and spyware infections</td>
<td>-0.29</td>
</tr>
<tr>
<td>Measure the effectiveness of security program components</td>
<td>-0.28</td>
</tr>
<tr>
<td>Ensure security program is consistently managed</td>
<td>-0.27</td>
</tr>
<tr>
<td>Know where sensitive or confidential information is physically located</td>
<td>-0.26</td>
</tr>
<tr>
<td>Secure endpoints to the network</td>
<td>-0.25</td>
</tr>
<tr>
<td>Identify and authenticate end-users before granting access to confidential information</td>
<td>-0.23</td>
</tr>
</tbody>
</table>

*Non-parametric correlation method utilized because of small sample size

...steps to achieve a governance infrastructure...

- a high-level individual...
- board-level oversight...
- adequate budget ...
- steering committee...
- Implement metrics that define program success
- senior executives reports...
appendix
State of Security Metrics

What leading security metrics companies report

• Number of security incidents (60%)
• Periodic measures of the risk posture (~50%)
• Business impact or the cost of incidents (>40%)
• Departmental achievement of security related behaviors (33%)
• Performance against Top 10 Vulnerabilities (30%)
• Financial losses suffered during a security incident (25%)

Executives Unhappy with Current Security Metrics
Mathew Schwartz (06)
## Operational Metrics

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viruses detected in user files</td>
<td>92.3%</td>
</tr>
<tr>
<td>Viruses detected in e-mail messages</td>
<td>92.3%</td>
</tr>
<tr>
<td>Invalid logins (Failed password)</td>
<td>84.6%</td>
</tr>
<tr>
<td>Intrusion attempts</td>
<td>84.6%</td>
</tr>
<tr>
<td>Span detected / filtered</td>
<td>76.9%</td>
</tr>
<tr>
<td>Unauthorized website access (content filtering)</td>
<td>69.2%</td>
</tr>
<tr>
<td>Invalid logins (failed username)</td>
<td>69.2%</td>
</tr>
<tr>
<td>Virus detected on websites</td>
<td>61.5%</td>
</tr>
<tr>
<td>Unauthorized access attempts</td>
<td>61.5%</td>
</tr>
<tr>
<td>Admin violations</td>
<td>61.5%</td>
</tr>
<tr>
<td>Intrusion successes</td>
<td>53.8%</td>
</tr>
<tr>
<td>Unauthorized information disclosures</td>
<td>38.5%</td>
</tr>
<tr>
<td>Span not detected</td>
<td>38.5%</td>
</tr>
<tr>
<td>Spam false positives</td>
<td>30.8%</td>
</tr>
<tr>
<td>Other</td>
<td>23.1%</td>
</tr>
</tbody>
</table>

(Slide Source: Information Security Program Metrics & The Balanced Scorecard, ISACA)

Effective Operational Security Metrics
Preventsys, Inc (05)