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
  - ISSA Blog: Pete Lindstrom “Do Security Metrics Matter?”
- 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

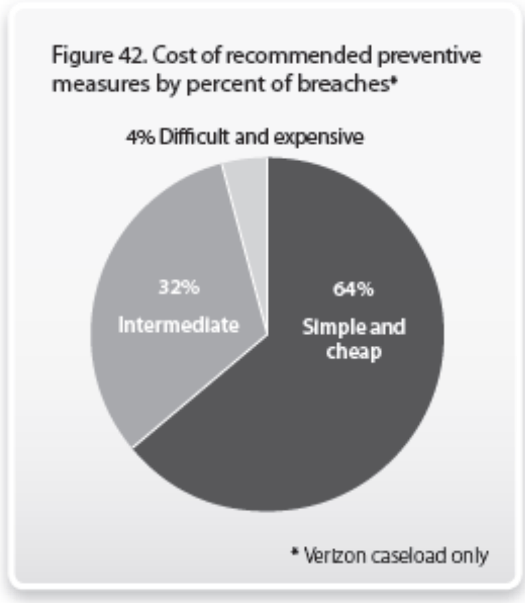
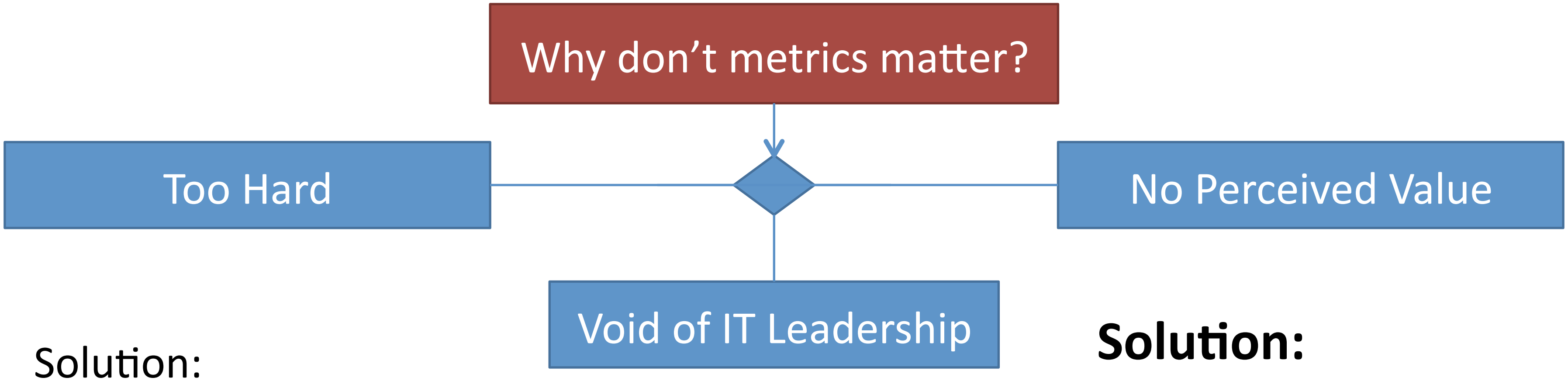


Figure 42. Cost of recommended preventive measures by percent of breaches*

* Verizon caseload only

VZ Breach Report 2010

Let’s Get It Going



Why don’t metrics matter?

Too Hard

No Perceived Value

Void of IT Leadership

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

Solution:

- **More evidence Metrics reduce loss**

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

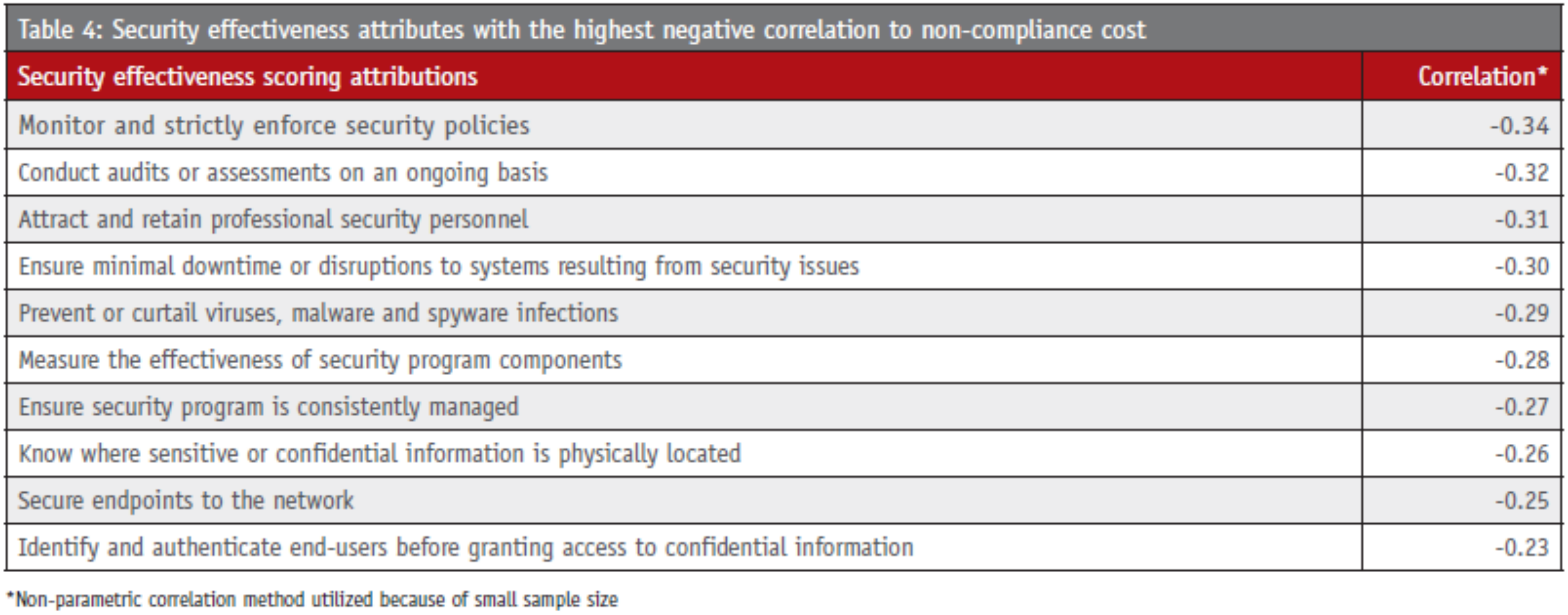


Table 4: Security effectiveness attributes with the highest negative correlation to non-compliance cost

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

*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

(slide source: Information Security Program Metrics & The Balanced Scorecard, ISACA)

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

Which of the following key data elements does your organization collect?	
Viruses detected in user files	92.3%
Viruses detected in e-mail messages	92.3%
Invalid logins (Failed password)	84.6%
Intrusion attempts	84.6%
Span detected / filtered	76.9%
Unauthorized website access (content filtering)	69.2%
Invalid logins (failed username)	69.2%
Virus detected on websites	61.5%
Unauthorized access attempts	61.5%
Admin violations	61.5%
Intrusion successes	53.8%
Unauthorized information disclosures	38.5%
Span not detected	38.5%
Spam false positives	30.8%
Other	23.1%

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

Effective Operational Security Metrics
Preventsys, Inc (05)