Bringing Metrics Into the Enterprise

Sandy Hawke, CISSP
Director of Product Marketing at BigFix

IT Just Works

Agenda

- Why Metrics?
- Why Not Metrics?
- What Security Can Learn from Operations
  - CIA has migrated to “all about the A”…
  - How to become efficiency experts
  - How to become the CFO “whisperer”
  - SLAs for Security
- Three IT Security Projects Your CFO *will* Approve
  - Their success is measurable
  - They save $$$
  - They improve security

The "Goodness" of Security Metrics

- When we measure, we can reward (or punish!)
- Drives accountability
- Raises awareness (aka need for security budget)
- Ties IT security to strategic business initiatives

"Face it, you've changed. The man I married would never subject his family to an annual cost-benefit analysis."

So… why haven't metrics been adopted?

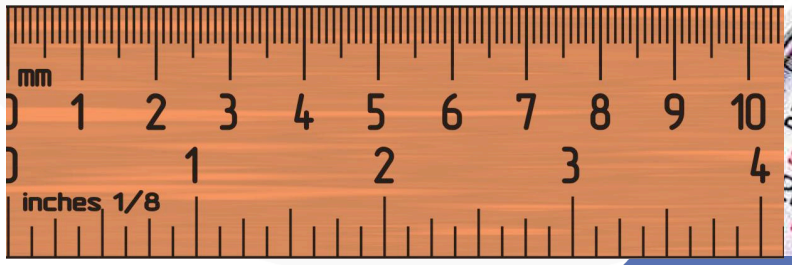
- Lack of consensus among stakeholders or industry
  - What's important? This answer depends upon your position within the enterprise or the security market…
- Lack of certainty, lack of visibility means lack of reliable data points to measure.
- Security team doesn't "own" the management of the solution

Operational Excellence in IT Security:
Some suggestions…

- View security with an operational filter.
- Start prioritizing the “A” in “CIA”
- Begin with a baseline by asking these questions:
  - What’s in my environment?
  - Which of these do I have control over?
  - Of these, which are in compliance with <insert standard here>?

Operational Excellence in IT Security:
Some suggestions…

- Develop methods and processes to measure efficiency in Change Management:
  - What percentage of the environment can we VERIFY conforms to these changes within a 24-hour timeframe? MAKE THAT YOUR SLA.
- Measure efficiency around auditing procedures (audit findings shouldn't be a surprise anymore)
  - How often do we monitor for non-compliance?
  - What's the process for remediation of non-compliant devices?
  - How long does it take from detection to remediation?



3 IT Security Projects to Propose:

Save $$, Be More Secure

1. Power Mgmt
   - ✓ Savings? $15 per managed asset rebate with no cap + what you save in actual energy cost.
   - ✓ Security? How? Desktops, laptops and servers that are turned off can't be infected or compromised…
2. Software application mgmt
   - ✓ Savings? Avoid inflated licensing fees, Use only what you know you need.
   - ✓ Security? Truly conservative configs (Don't need it? Remove!)
3. Infrastructure consolidation
   - ✓ Savings? Reduce # of consoles, reduce # of FTEs to manage them.
   - ✓ Security? Overworked admins = mismanaged systems = increased risk. Plus, how do you know root cause of an incident?

Requirements for Metrics

- ✓ Measurable / demonstrable
  - ✓ “I just feel more secure” doesn’t hold weight
- ✓ Relevant
  - ✓ Across time parameters
  - ✓ Tied to strategic business objectives
- ✓ Simple and accessible
  - ✓ Across disciplines
- ✓ Actionable
  - ✓ Make sure remediation steps are clear *and* possible
- ✓ Easily transferable between roles

Summary

- Getting your IT security project approved is a good thing
  - Use metrics to make the case
- Key requirements for getting security projects approved:
  - Know what you have
  - Demonstrate that “X” project will produce “Y” result
  - Measure improvement over time