Is this as prevalent as we fear?
Security Metrics: Leading Indicators for Adoption

- **Who**
  - Just ‘top tier’ companies?
  - Who is the primary sponsor?
  - Who generates metrics and scorecards?
  - Who is the audience?

- **Why**
  - Drive improvement, justify budget, prioritize investments,
  - Prove compliance, manage risk, security group PR

- **What**
  - What metrics are most useful?
  - What resources are being allocated to measurement?

- **Where**
  - Sources of raw data
  - Mechanisms for publication of results

- **When**
  - Daily, weekly, monthly, quarterly?
  - Other regular reviews that security metrics would be included

- **How**
  - Tools: Excel, Data Mining Products, Report Writers, Point Products
  - People: Formally assigned or ad hoc
State of Metrics Adoption in 2006

- Maturity based upon:
  - Regularity, repeatability
  - Consistency, trust
- Low maturity across the board: \( \rho_{x,y} = 0.22 \)

Companies Surveyed

- 56%: Over $100B
- 26%: $50-100B
- 18%: Under $50B

Metrics Maturity vs Market Cap ($B)
Why and When

- Compliance is not the first application of metrics
- Early adopters in financial services
Why are Metrics so Hard?

- Vast and unclean data
  - Scattered and uncorrelated
  - Incomplete and inconsistently collected
- Lack of consensus on indicators and models
  - Statistics
  - Aggregation
- Difficult to package results
  - Mapping to business
  - Multiple audiences
  - Visualization of quantitative data
  - Distribution
Metricon 1.0: Enterprise & Case Studies B

- John Nye: Leading Indicators for Vulnerabilities
- Vik Solem: Top 10 Vulnerabilities over Time
- Jonas Hallberg: Metrics for Networked Info Systems
- Andrew Sudbury: Highlights of a Security Metrics Scorecard Project
How decisions are made

1-2-3

Rock! Scissors!

Your project is approved... unless scissors can't cut rock.

Assume it's sheet rock.