What are “security metrics”

- Very wide variety; a few examples:
  - Number of port scans on one or more servers
  - Number of stolen laptops
  - Number of password lockouts on an application due to repeated failed attempts
  - Number of people who have failed to take required security training
  - Number of servers running with known security vulnerabilities

What to do with them?

- Compare results with other organizations
  - Assumes metrics are comparable
  - Look for differences which may suggest “out of alignment” with norms
  - Let results “speak for themselves” (no one wants to be at the back of the pack)
- Compare results over time – look for trends
- Use as an “indicator” in the hands of security professionals to make security-related decisions
  - Like doctors use diagnostic testing results to make healthcare decisions

What NOT to do with them?

- Use them as performance imperatives, so work focuses on trying to “move the meter”
  - In essence, that which is measurable takes higher priority that than which is not
  - Panmunjom problem – argument over “shape of the metrics” rather than over substance
- Corollary: create specific requirements
  - Require % reduction (or increase) per year – usually inadvisable
- Measure overall security “status” of organization at a point in time
  - Relating metric to risk is fraught with problems

Path Forward

- Try to get agreement on common metrics with other organizations – including willingness to share metrics
  - Private companies can do privately
- Keep alert to data which suggests that a metric may be quantifiably related to a specific risk
- Look for trends over time – and take action if the trends appear to be problematic

Final Observations

- Security metrics are akin to “return on investment” debate
- There are lies, damned lies, statistics, and then ROI calculations
- We should not let the natural hunger for quantitative data drive us to bad decisions
- Remember that even Lord Kelvin – Mr. Quantitative - was convinced that “heavier than air flying machines are impossible…”