Metricon 4.0

The Importance of Context

On the topic of context:

- Nye pointed out that security measurement must become reproducible. If risk assessment is subjective, then like judging figure skating or humanities papers, in security measurement “subjectivity should be baked into the measurement standard.”
- Ellam told us that if threats to security are dynamic (and they are), then countermeasures must be dynamic.
- McGraw characterized a metrics program as “like an organ,” in that “transferring a metrics program from one enterprise to another seems much like organ transplant — chances of rejection by the host are high.”

Some contextual findings:

- Bellis' noted that in the face of complexity, automation is flatly essential and that that automation has as its purpose action plans and their management, yet at the same time one aspect of rising complexity: that less and less of the environment is subject to an effective snapshot.
- Clark said that all software enjoys a honeymoon: The time it takes an attacker to learn a piece of software, find its bugs, write, debug & test an exploit, and release it into the wild.
- Nichols showed that there is little-to-no lasting effect on market equity (stock price) due to a data breach.

Session topics meant different things in context of different presentations:

1. Baseline Scoring Methods – inadequacy of existing controls versus measurement of existing controls
2. Measuring Impact - monetary versus system performance
3. Enterprise Security Management - GRC, CIP, EEE

Lunch over discussion of six different topics with facilitators and handouts

4. Software Security - code quality versus honeymoon periodicity
5. Trends and Stats - data breach incidents in themselves versus their impact on stock price
6. Security Manager Panel - debate over when risk acceptance is illegal

Some attendee feedback:

What questions did you get resolved?

- *Who is working on what.*
- *Lay of the land.*
- *What the current questions are.*

What new questions did Metricon generate for you?

- *A lot of questions centered around measuring risk from one company to another.*
- *How to get others to care (i.e. C-level). Impact analysis.*
- *How to work together.*