Security Metrics in Industry: Results from Workshops and Field Studies

Scott Dynes, M. Eric Johnson

Center For Digital Strategies,
Tuck School of Business at Dartmouth College

Eric Goetz

Institute for Information Infrastructure Protection

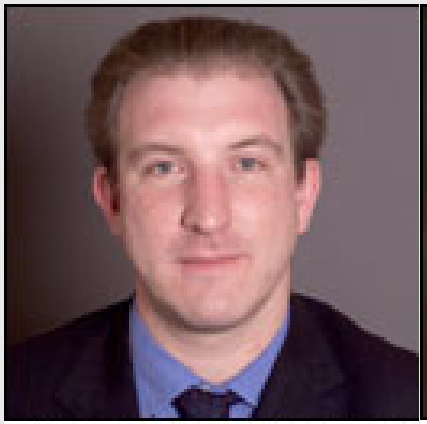
Mini-Metricon April 2008

This material is based upon work supported by the U.S. Dept. of Homeland Security under Grant Award Number 2006-CS-001-000001, under the auspices of the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, or Dartmouth College.

A Workshop on Security through Information Risk Management (2007)

- Ranking the Risks
- Communicating the Risks
- Preparing the Organization
- Measuring Progress

Gregory Garcia, Assistant Secretary, Cyber Security, U.S. Homeland Security



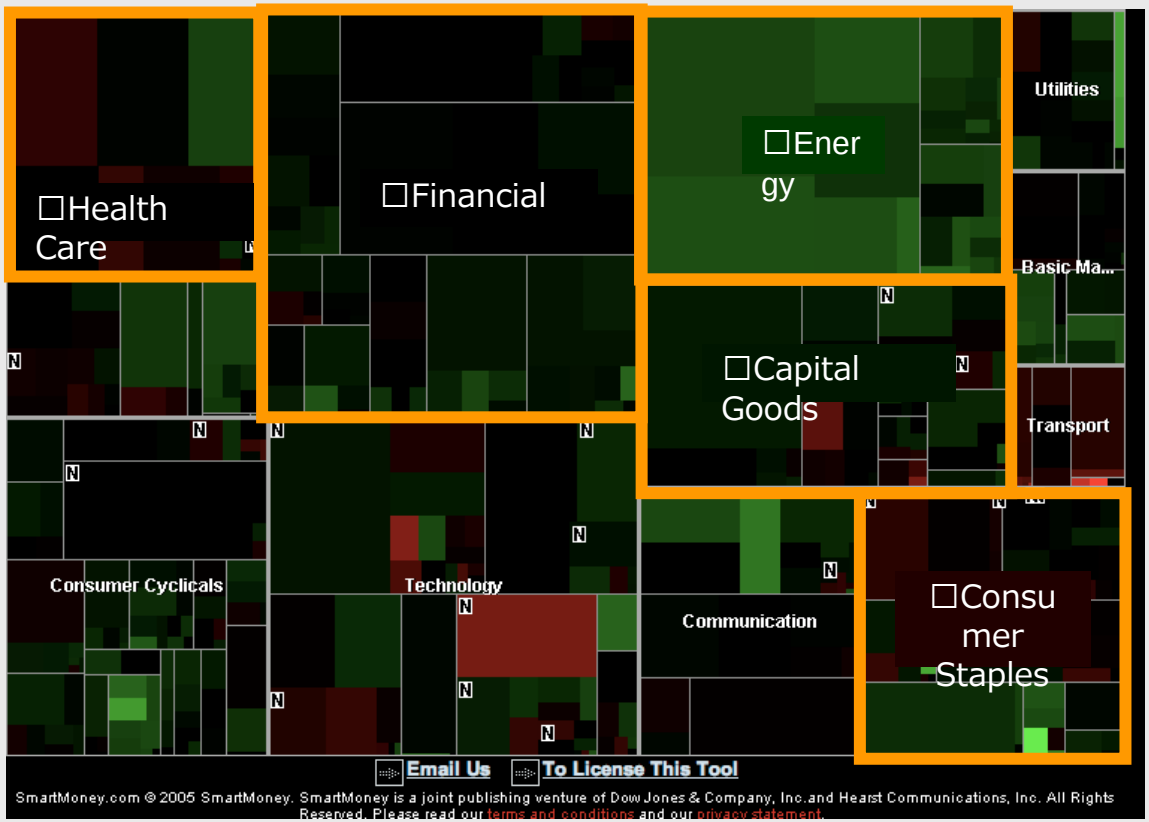
Phil Venables, Managing Director and CISO, Goldman Sachs

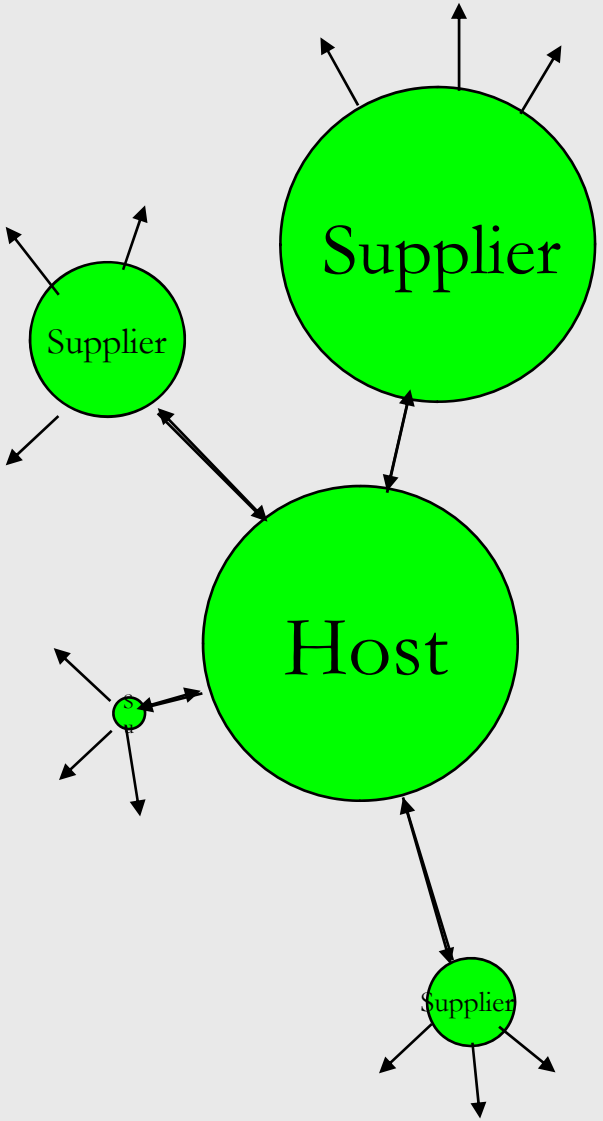
John Stewart, VP, Corporate Security Officer, Cisco Systems

Thor Geir Ramleth, SVP and CIO, Bechtel Group, Inc.

Tuck Business Rationale Field Studies

Focus: How Firms Identify and Manage Information Risk





What metrics are being used?

-Checklists, scorecards

Provide percentage score, but hard to prove validity/effectiveness

- Composite metrics

Provide risk score, provide affordances for easily understanding security stance

- Regulatory regimes (PCI, SOX, etc.)

- $$ impact of potential InfoRisk events

Tying everything to $$ makes ranking, investing easy

Use of Metrics

- Motivating change to move the Info. Risk Mgmt. needle
  - Cisco: weekly call with VPs laying out InfoSec performance for last week
  - Top 300 executives at BOA have half their compensation ties to performance on a composite security metric
  - Security dashboards
- Measuring whether IR education efforts effective
  - Firms correlate security training and testing scores, audit findings, actual security breaches and events, and security behavior of individuals, to come up with a composite score.
  -Cisco: Bonus depends on InfoSec training
- Benchmarking

Downsides to security metrics

- Folks manage to the metric:

"Measurement becomes an abdication of personal responsibility."

- Lack of responsiveness to future threats:

"…how do we measure the emerging threats?"

Take-Away: The Arc of Security Metrics

- Metrics were seen as being core to InfoSec efforts…

… and then (now) were (are) seen as part of current practice, but firms are seeing limitations…

… leading to a new approach using applications helping firms to identify and manage IT-based business risk (Archer Technologies, RiskWatch, and SecureCompass).