HOMELAND SECURITY STUDIES & ANALYSIS INSTITUTE

An FFRDC operated by Analytic Services Inc. on behalf of DHS

Measuring Cybersecurity Information Sharing

Matthew H. Fleming, Ph.D.

27 February 2012

This research sought to answer the following question: what metrics should be used to gauge the efficacy of cybersecurity info sharing?

- Efforts to secure and defend public- and private-sector systems rely in part on information sharing on cyber threats and vulnerabilities
- But information sharing is not cost-free—though unlikely, it may, theoretically, not be the best use of scarce resources
- This begs the question: How do we know if info sharing is effective?
- Accordingly, the research sought to identify a suite of metrics to measure performance in cybersecurity information sharing

The research turned to first principles (and literature) to answer the rsch question by considering the definition of information sharing itself

- Information sharing represents the process through which information is provided by one entity to one or more other entities to facilitate decision-making under conditions of uncertainty, where:
  - Information represents “data + meaning” (Floridi 2009)
  - Decision-making represents goal-directed behavior in the presence of options (adapted from Hannson 2005)
  - Uncertainty represents the state of being uncertain (i.e., not known; indeterminate; questionable; variable; adapted from Merriam-Webster 2002)

The definition of information sharing carries with it some important implications for the selection of metrics

- Information sharing should be goal-directed
- Information should be shared w/entities who can effect/affect achievement of goal—but not with those who cannot
- Shared information should be used for purposes that can effect/affect achievement of goal—but not other purposes
- Shared information should be fit for the purpose of reducing uncertainty
- Info sharing cannot reduce all uncertainty (sometimes it may increase it)

The definition and its associated implications drive the selection of metrics concepts (for which there are one or more specific metrics)

Inputs	Processes	Outputs	Outcomes
Shared information = data + meaning Shared info is relevant Shared info is timely Shared info is accessible Shared info is accurate	Goal is specified Goal is agreed Entities are appropriate Entities are participating No loss of control No information overload Entities are sufficiently resourced/trained	Shared information is used for both tactical and strategic purposes	Goal is achieved

Questions and coordinates

- I’d be happy to answer any questions
- My coordinates:
  - Matthew H. Fleming, Ph.D.
  - Fellow, Homeland Security Studies and Analysis Institute
  - T: 703-416-3471
  - E: matthew.fleming@hsi.dhs.gov