CYBER SECURITY DIVISION

2013 PRINCIPAL INVESTIGATORS’

Improving CSIRT Skills, Dynamics and Effectiveness

Shari Lawrence Pfleeger (Dartmouth), Lois Tetrick (GMU), Steve Zaccaro (GMU), Reeshad Dalal (GMU), Bill Horne (Hewlett-Packard)

17 September 2013

Homeland Security

Science and Technology

Team Profile

- **George Mason U**: Organizational psychologists looking at
  - knowledge, skills and abilities;
  - teams;
  - interactions
- **Hewlett-Packard**: Runs Navy-Marine Corps Intranet (NMCI); will provide access to
  - NMCI CSIRT, network analysts, help desk, etc. (NMCI is the largest internal computer network in the world: 363,000 computers, 707,000 sailors, 620 locations)
  - Other CSIRTs
  - Perform process modeling
- **Dartmouth**: Project management; Will analyze costs and benefits
- **Primary customer**: US-CERT

Customer Needs

DEFINE EFFECTIVENESS
What do we mean by an effective team? By an effective team member?

CSIRT PROCESSES
What should CSIRT members do, when and for how long?

TECHNOLOGY AND DECISION SUPPORT
How can we implement what we now know?

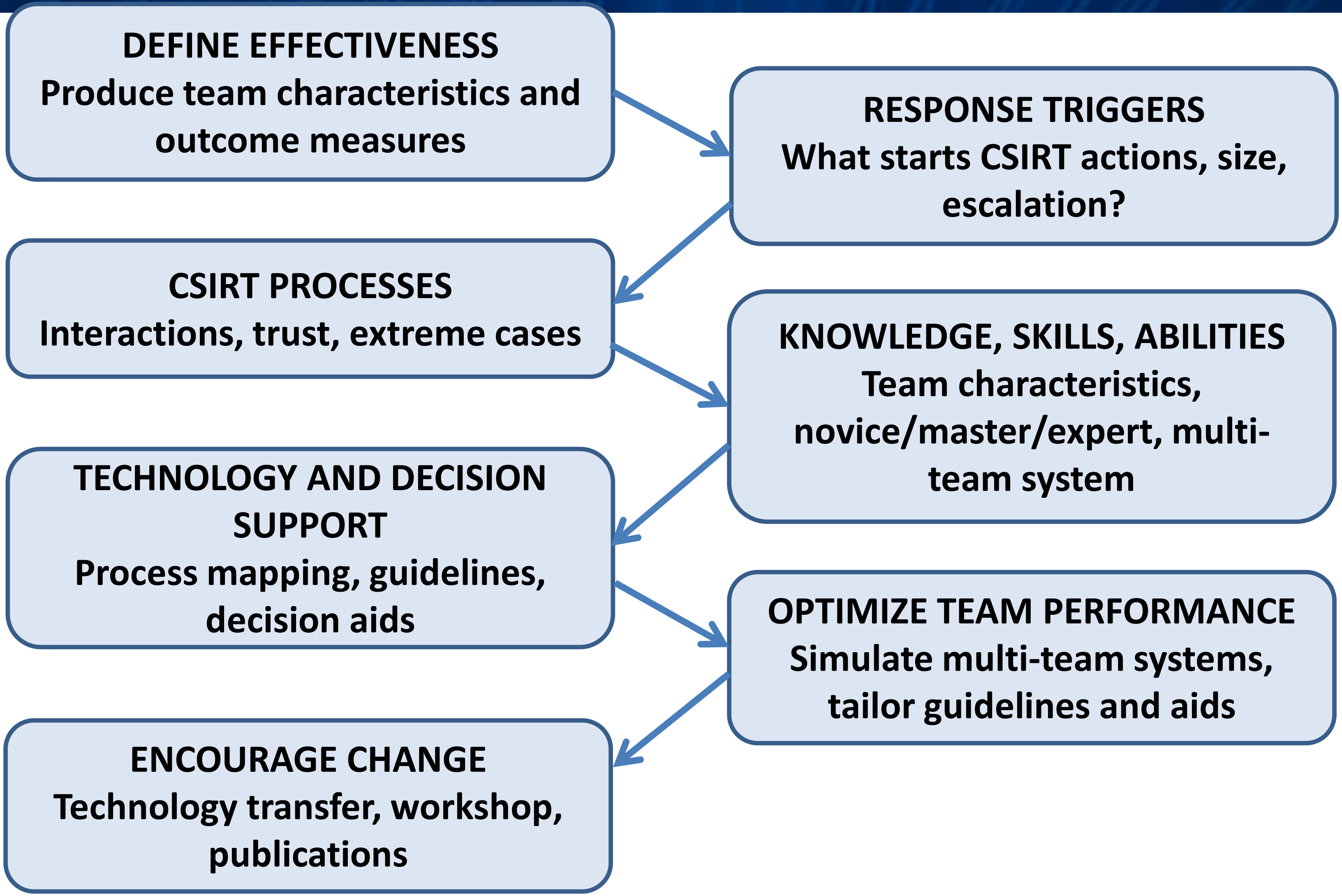
ENCOURAGE CHANGE
How do we encourage change from within? From without?

RESPONSE TRIGGERS
What starts CSIRT actions, size, escalation?

KNOWLEDGE, SKILLS, ABILITIES
What are the team characteristics? How do we tell novice/master/expert? What other teams are involved in this multi-team system?

OPTIMIZE TEAM PERFORMANCE
How do we encourage best performance?

Approach



DEFINE EFFECTIVENESS
Produce team characteristics and outcome measures

RESPONSE TRIGGERS
What starts CSIRT actions, size, escalation?

CSIRT PROCESSES
Interactions, trust, extreme cases

KNOWLEDGE, SKILLS, ABILITIES
Team characteristics, novice/master/expert, multi-team system

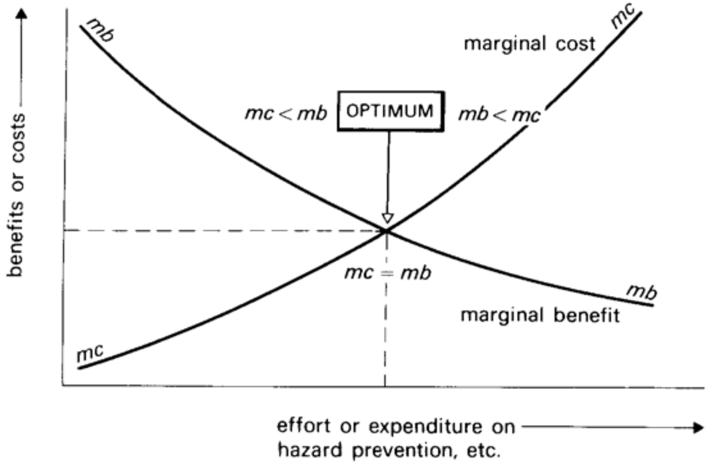
TECHNOLOGY AND DECISION SUPPORT
Process mapping, guidelines, decision aids

OPTIMIZE TEAM PERFORMANCE
Simulate multi-team systems, tailor guidelines and aids

ENCOURAGE CHANGE
Technology transfer, workshop, publications

Benefits

- Enables best use of resources, especially people
- Encourages flow from novice to master to expert
- Provides back-up capabilities and trains newbies
- Provides measurable criteria for improvement
- Balances security needs with other organizational needs, including economic ones



Current Status

- Literature review
- Taxonomy of CSIRT processes and activities (individual, team, MTS)
- Focus group and individual interview protocols

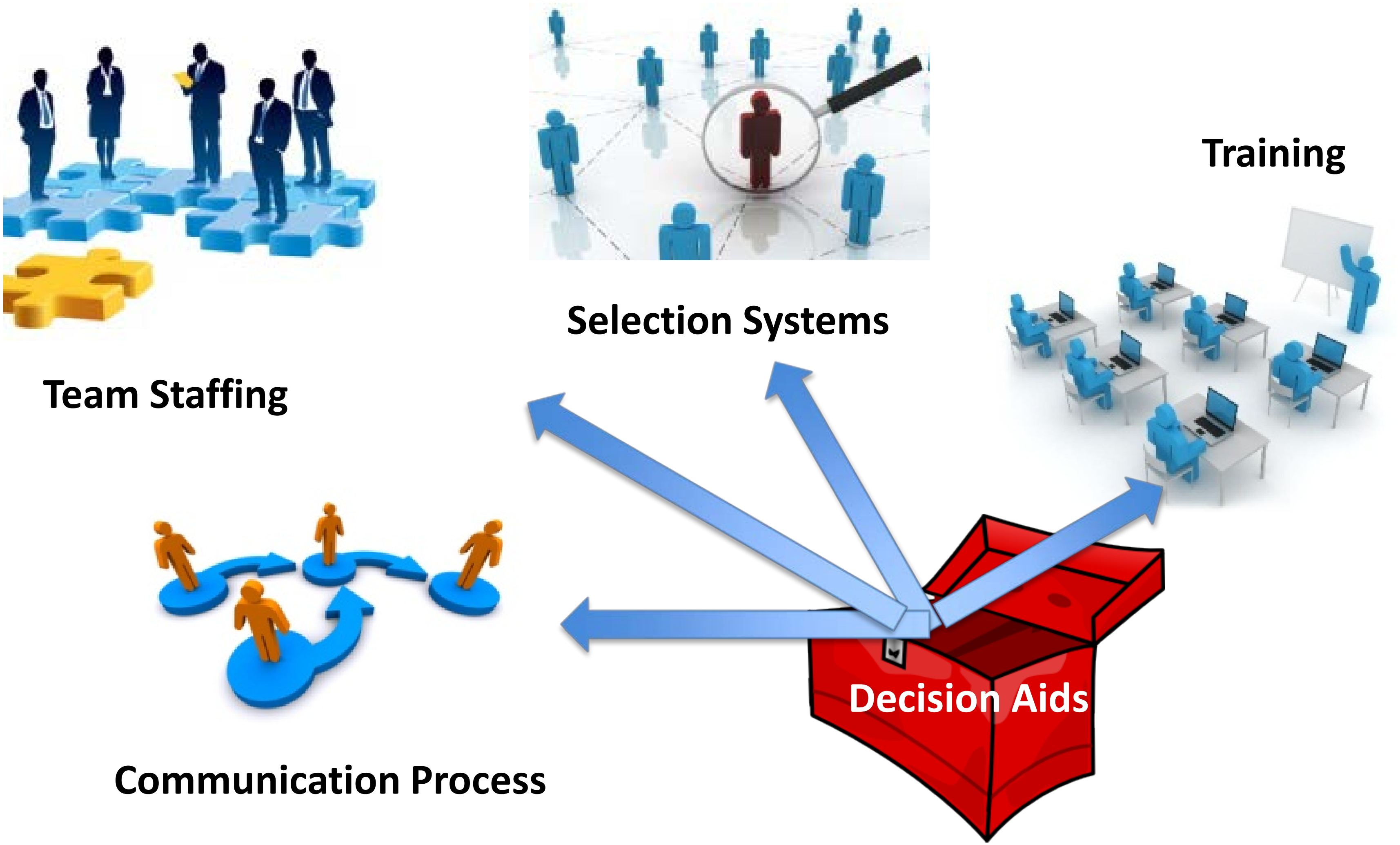
- Visits to NMCI, HP ES
- Planned visits to other sites

- Review of NICE categories
- Data analysis on-going
- Planning inclusion of Swedish and Dutch CERTs

… Informs Identifying Knowledge, Skills and Abilities

… which in turn

… Will Inform Tools Designed to Improve Selection, Training and Process



Team Staffing

Selection Systems

Training

Communication Process

Decision Aids

Next Steps

Deliverable	Progress Made	Expected
Interview US-CERT	Will hold discussions on availability	Early 2014
Economic model	On hold. Coordinating with University of Maryland task.	Late 2014
Description of classes of CSIRT processes for types of teams involved	Initial review of research-based literature Consideration of nature of process modeling	Dec 2013
Documentation of CSIRT roles and responsibilities, team-member influence, and knowledge, skills and abilities of individuals and team	Conducted contextual performance analysis and cognitive task analysis at HP ES to begin identifying KSAs of individuals Conducted individual task analysis using survey techniques at HP Enterprise Services	May 2014
Initial guidelines for CSIRT creation and management	Scheduled focus groups and individual interviews with newly forming HP Global Security CSIRT	Nov2014
Decision aids for CSIRT tailoring		Nov 2014
Updated guidelines, informed by optimization results		June 2015
Recommendations for individual member, team and MTS selection, staffing, training, and performance management		June 2015
CISO workshop to disseminate results	This task is on hold with economics task.	Sep 2015
Evaluation of technology demonstration in an operational environment		Sep 2015

Contact Information

- Project Lead: Shari Lawrence Pfleeger (pfleeger@dartmouth.edu)
- GMU Lead: Lois Tetrick (ltetrick@gmu.edu)
- HP Lead: Bill Horne (william.horne@hp.com)