27th ANNUAL

FIRST CONFERENCE BERLIN

14-19 JUNE 2015

UNIFIED SECURITY: IMPROVING THE FUTURE

BARRIERS AND PATHWAYS TO IMPROVING CSIRT EFFECTIVENESS: INFORMATION SHARING

Presented By:

Kristin M. Repchick, M.A.

Julie Steinke, Ph.D.

Laura Fletcher

GEORGE MASON UNIVERSITY

Workshop Overview

Project funded by the U.S. Department of Homeland Security, Science & Technology Directorate (BAA 11-02)

Contact:
Scott Tousley

Collaborators

National Cyber Security Centre
Ministry of Security and Justice

Contact:
Kas Clark

MSB
Swedish Civil Contingencies Agency

Contact:
Richard Widh

Workshop Overview

<u>Other Team Members</u>

Stephen J. Zaccaro, Ph.D.

Lois E. Tetrick, Ph.D.

Reeshad S. Dalal, Ph.D.

Tiffany R. Chen, Ph.D.

Amber Hargrove, M.A.

Carolyn J. Winslow, Ph.D.

Kristin M. Repchick, M.A.

Daniel Shore, M.A.

Alan J. Tomassetti, M.A.

Aiva Gorab, M.A.

Jennifer Green, M.A.

Balca Bolunmez

Laura Fletcher

Ziton Sheng, M.A.

Qikun Niu, M.A.

Shannon Schrader

George Mason University

Research Team

Dartmouth College

Shari L. Pfleeger, Ph.D.

Hewlett-Packard

William G. Horne, Ph.D.

Sandeep N. Bhatt, Ph.D.

Loai Zomlot, Ph.D.

Session Roadmap

Effective Information Sharing

Differing Perspectives

Developing Connections

Roadblocks

Session Objectives

- Understand and describe various perspectives on information sharing
- Facilitate effective information sharing
- Develop and implement strategies to enhance cybersecurity information sharing

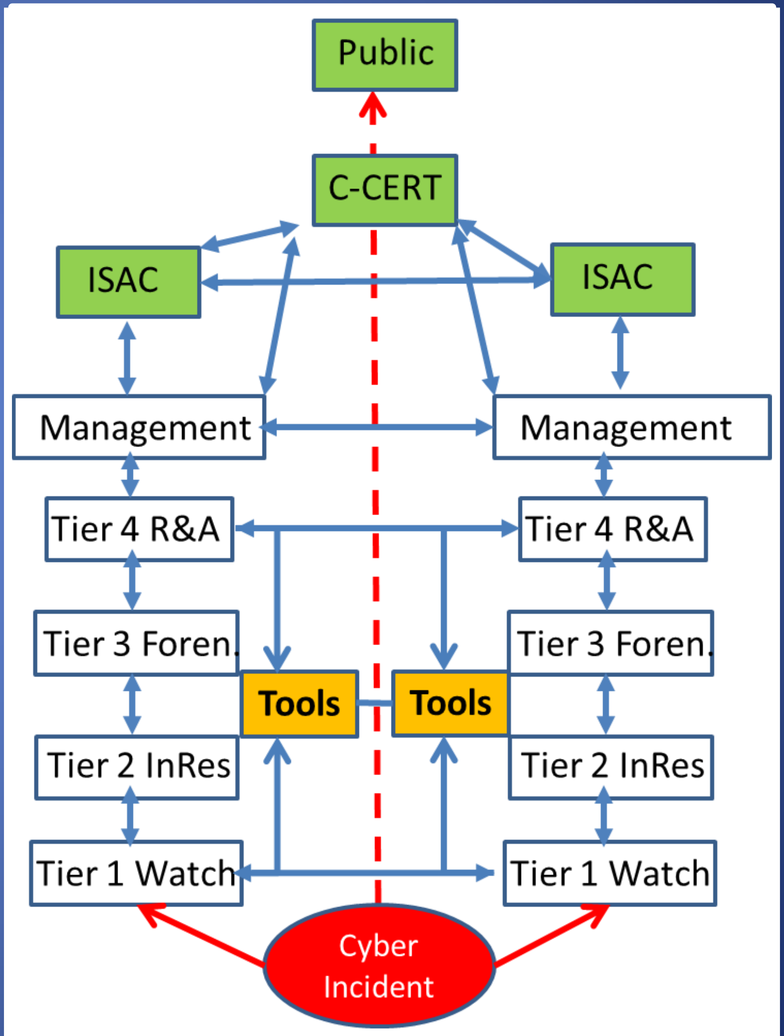
Perspectives on Information Sharing

Cybersecurity Domain

Perspectives on Information Sharing

Cybersecurity Domain

- Questions:
  - – Obstacles within and between levels?
  - – Incentives to information sharing?



Perspectives on Information Sharing

Organizational Psychology

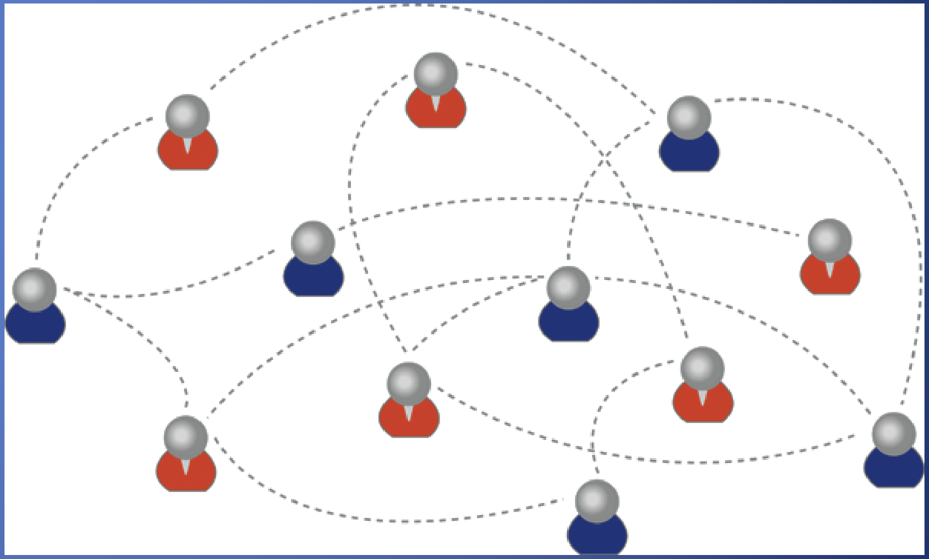
- **Conscious** and **deliberate** attempts ...to **exchange** work-related information
- "Making statements to other group members about a **task**"

Bunderson & Sutcliffe (2002, p. 881)
Jehn & Shah (1997, p. 777)

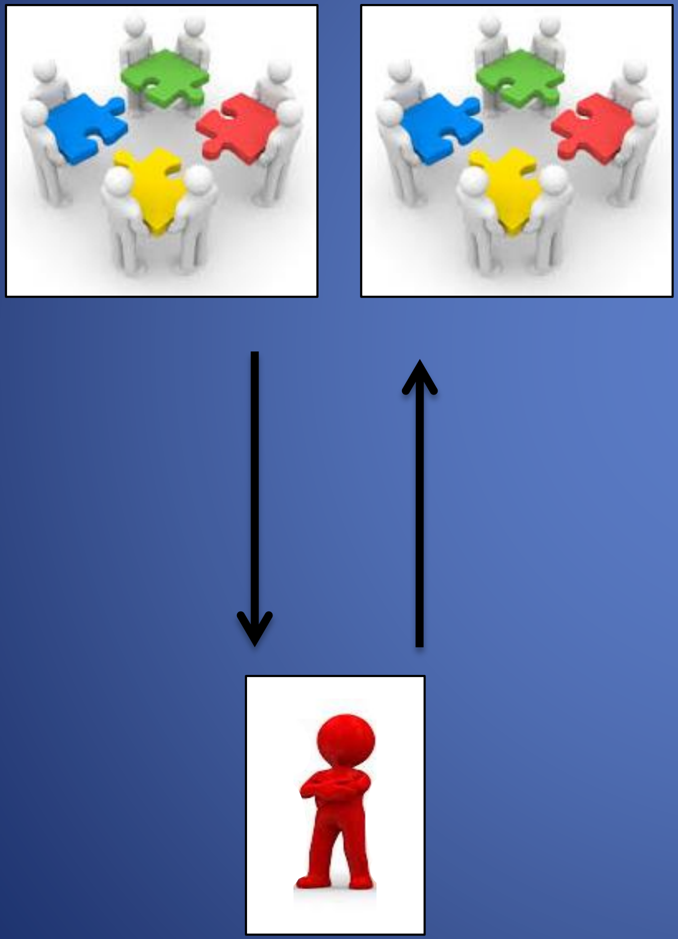
Perspectives on Information Sharing

Organizational Psychology

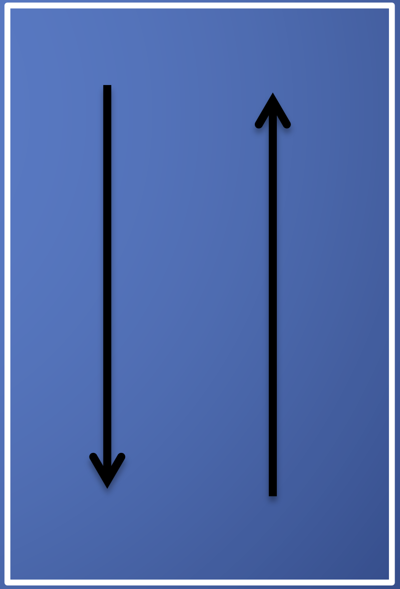
- **Within a team**
  - Coworkers, leader-subordinate
- **Between teams**
  - Different specialties/functions
- **Between external teams**
  - Examples:
    - Other business units
    - Clients
    - Other CSIRTs
    - Law enforcement



Perspectives on Information Sharing



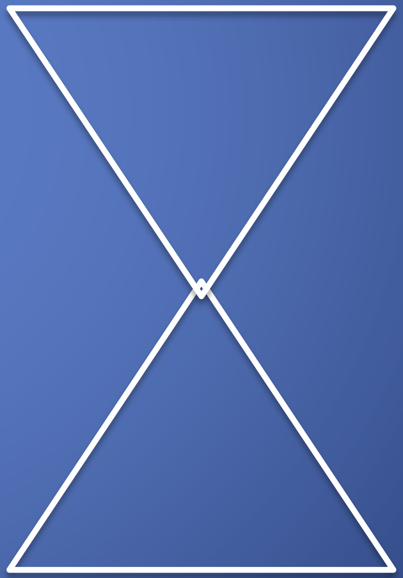
Multiple Teams & Agencies



Individuals

Perspectives on Information Sharing

Multiple Teams & Agencies



Individuals

ORGANIZATIONAL PSYCHOLOGY

What is Information Sharing?

- Many forms
  - Handoff
  - Public Announcements
  - Data
    - Specific threats
    - Indicators of compromise

Organizational Psychology

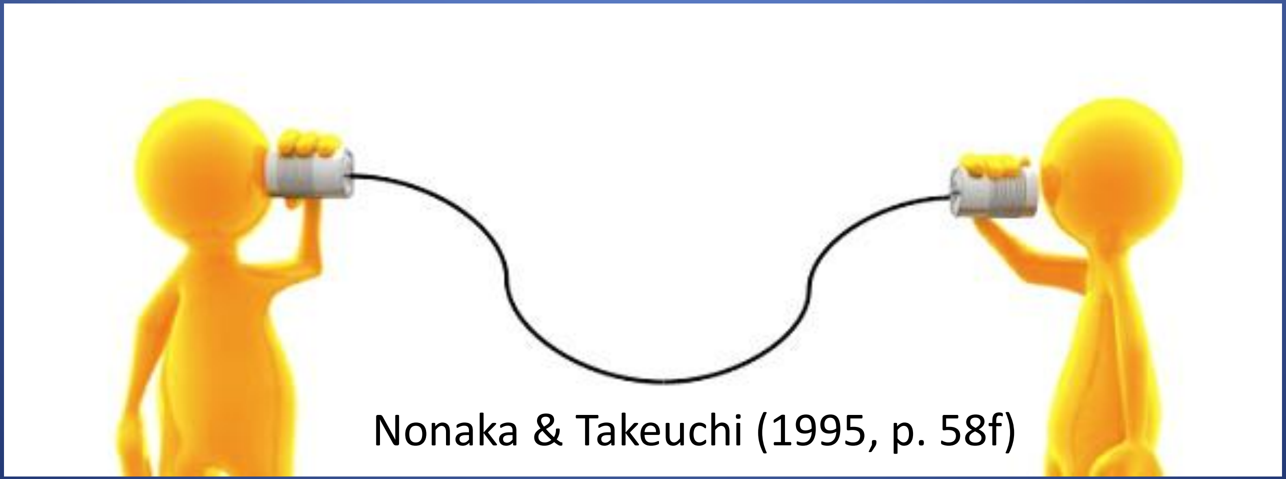
“And if you’re not on duty but some other guy is, he can see okay, this is related to this incident. I didn’t see any information. Let’s send a reminder or get some information. So **it’s done in the daily handover of routines**. So it is not just between the teams, but at this moment it is already done between the members.”

~ CSIRT Focus Group Member

ORGANIZATIONAL PSYCHOLOGY

How is Information Sharing Different?

- **Knowledge sharing**
  - – Information = **content** of messages
  - – Knowledge = **created** by flow of information
    - Anchored in the beliefs and commitment



Nonaka & Takeuchi (1995, p. 58f)

Organizational Psychology

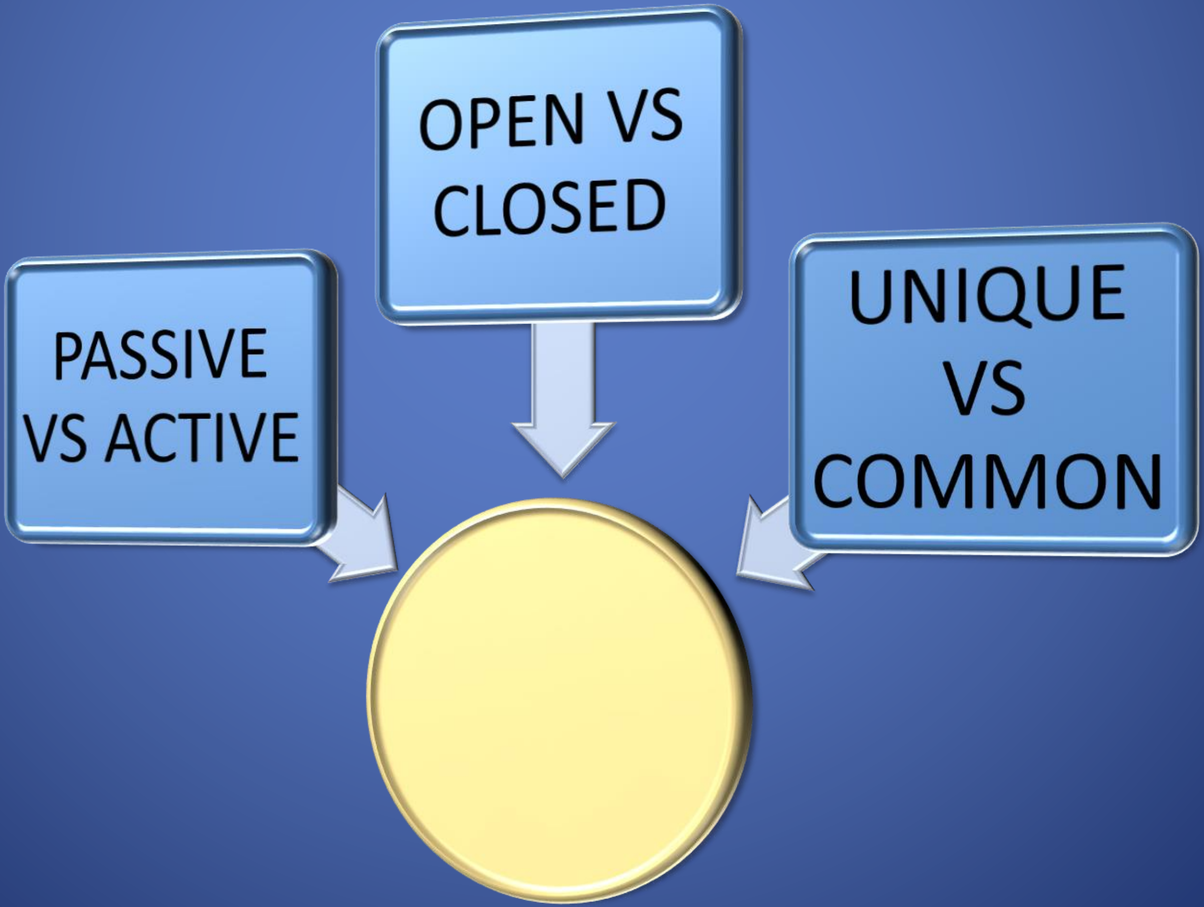
Why Information Sharing **Within** and **Between** Teams is Important

- Effective information sharing **enhances knowledge**

- CSIRTs are **KNOWLEDGE TEAMS**
  - Good information sharing skills increase effectiveness

Organizational Psychology

- How Does it Work?



PASSIVE VS ACTIVE

OPEN VS CLOSED

UNIQUE VS COMMON

Organizational Psychology

PASSIVE	ACTIVE
Posting or asking for information, opinions, or suggestions **Examples:** logs, wiki posts	Active task behavior – offering opinions, suggestions, and information **Examples:** debriefing, discussing an event/incident

Organizational Psychology

OPEN	CLOSED
The extent to which a team overtly shares information Volume of information shared Generates common knowledge	Limited or no information sharing, either due to lack of awareness of what should be shared or unwilling to share information

Organizational Psychology

UNIQUE	COMMON
Typically unshared information (unique to one source) May go against common information and knowledge Could impact group decisions if known ***Less likely to be shared***	Easily shared information Verifies common information & knowledge within a team or group Common knowledge effect / information sampling bias ***More likely to be shared***

Organizational Psychology

Why Good Information Sharing is Important

- Unique Information
  - Improved problem-solving
  - Increased creativity
  - Better decision-making
  - Enhanced strategies
- Open Information
  - Increased:
    - Team satisfaction
    - Cohesion
    - Trust

Information Sharing:

- Develops shared understanding of situations
- Leads to shared expectations about what information should be given or received in that particular context

ORGANIZATIONAL PSYCHOLOGY

Roadblocks to Information Sharing

- Information **overload**
  - Having more information than you can absorb

Situational Awareness

- Information **loss**
- **Wrong** information
- **Misclassified** information
- **Late/delayed** information

- **Checklists**
- **Clear Standards for procedures and processes**

ORGANIZATIONAL PSYCHOLOGY

Roadblocks to Information Sharing

- **Unavailable/missing** unique information
  - Missing cues during an incident
- Not knowing **who needs or has** the information
  - Or who should receive information

- **Backup behaviors**
- **Asking questions**

Increasing Shared Knowledge of Unique Expertise

Organizational Psychology

Roadblocks to Information Sharing

- **Sharing false information on purpose**
- Knowledge **hiding**
  - Deliberate withholding of knowledge requested by others
  - Driven by individual motivations / goals
  - **Classification of incidents** can impact information sharing

Develop an Open Culture

Organizational Psychology

What Inhibits Information Sharing?

- Among **Individuals**
  - Motivation, personality
- At the **Team** Level
  - Team type (e.g., virtual)
  - Ingroup-outgroup biases
  - Diversity
  - Team maturity
  - Team climate (trust & psychological safety)
  - Time pressure

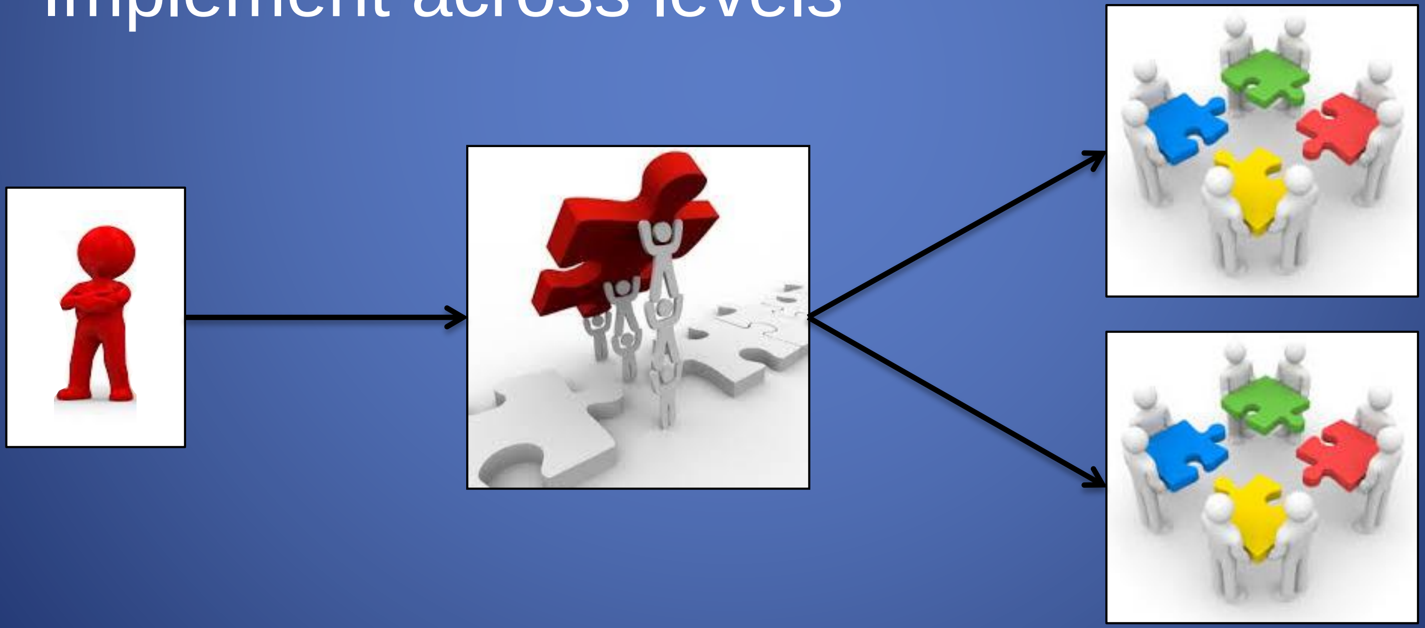
ORGANIZATIONAL PSYCHOLOGY

What Inhibits Information Sharing?

- **Organizational** Level
  - – Fear of negative impact:
    - Brand / public image
    - Legal issues
    - Stock price
  - – Hierarchical structures
  - – Overly restricting rules
  - – Socio-cultural barriers
  - – Climate
- Between organizations...

STRATEGIES!

- Empirically Based Strategies from Organizational Psychology can help!
  - Implement across levels



STRATEGIES!

Enhance Task Related Processes

- Define the task
  - Determine if “right” answers exist
- Define Processes
  - Facilitate structured discussions
  - 1-4 minute debriefings
- Create or maintain a wiki or virtual whiteboard
- Handoff checklist with clear responsibilities for each step in the process
  - Mnemonics (e.g., SBAR and SHARED)

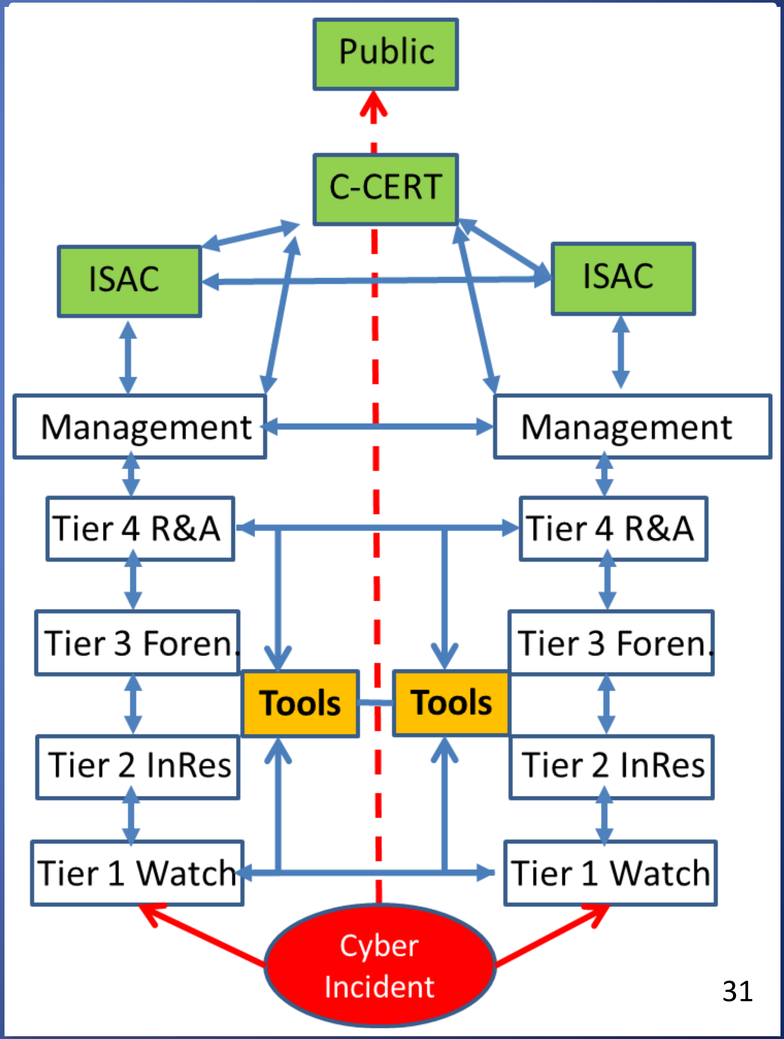
Haig & Whittington (2006)
Pham et al. (2012)

STRATEGIES!

Consider Team Characteristics

- Establish climates of trust and learning
  - Consider locations of team members*
  - Use After-Action-Reviews (collaborative)
- Clearly define team roles
  - Create a knowledge catalogue
- Have a designated “boundary spanner” to share information with other teams
- Promote unique information sharing
  - Ask for other’s ideas, have people prepare solutions independently before sharing with the group

Let's Share Information!



Interested in more information or participating in our research?

Contact Information:

Julie Steinke
jsteinke@gmu.edu

Kristin Repchick
krepchic@gmu.edu

Laura Fletcher
fletch5@gmu.edu

Thank You for Participating!

Vielen Dank für
ihre teilnahme!

Focus Group Quotes

"You have **formal and informal [networks]**... What you see … is that at the operational level, there is a lot of sharing going on that is informal. It becomes formal when you start making agreements for something. Then you have a formal agreement to share information, but most of the information is shared along a formal base because they are operational people."

~ CSIRT Focus Group Member

Focus Group Quotes

“You don't remember a lot from a report from six months ago. But you are not alone. We are 10. If you see something and you saw it within the group, there's a big chance one or two will answer, "Oh, it was that.
You can find information there."

~ CSIRT Focus Group Member

Focus Group Quotes

"I guess your information is formally correct, but we also do a lot of discussing among ourselves. So when there is an incident and if we have any doubt or need any advice, we always talk to each other. It depends, of course, on the classification of information.

We use the traffic light protocol to decide what information can be disclosed within the organization, or if it's just for your ears only, it can be based as well and it's more difficult. But normally, cases can be discussed."

~ CSIRT Focus Group Member

Focus Group Quotes

“We discuss incidents in small groups or sometimes with the whole team …one of the positives of our team is that **anything can be discussed, and we really help people interact with each other and discuss** – okay, this is the situation; I’m not sure what to do. And just by the discussion itself – oh, maybe this is the right direction to go to.”

~ CSIRT Focus Group Member

Focus Group Quotes

"We'll put out current activity … when there's updates I want people to keep their stuff up to date. If there's some kind of phishing scam or something that's widespread just that people are aware of it, that can come to our website and look at it, get some background, or somewhere else to get a big more information on it. And then there's also some weekly things we do, like vulnerability summaries for the past week that go out."

~ CSIRT Focus Group Member