



27<sup>th</sup> ANNUAL  
**FIRST** **BERLIN**  
CONFERENCE

14 - 19 JUNE 2015

**UNIFIED SECURITY:  
IMPROVING THE FUTURE**



# Barriers and Pathways to Improving CSIRT Effectiveness: Information Sharing

*Presented By:*

Kristin M. Repchick

Laura Fletcher

Julie Steinke



# Information Sharing Topics



# What is information sharing?

- “**Conscious** and **deliberate** attempts on the part of team members to **exchange** work-related information, keep one another appraised of activities, and inform one another of key developments”
- “Making statements to other group members about a **task**”



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

# What is information sharing?

- Can take many forms
  - Handoff
  - Public announcements
- CSIRT example
  - “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.”



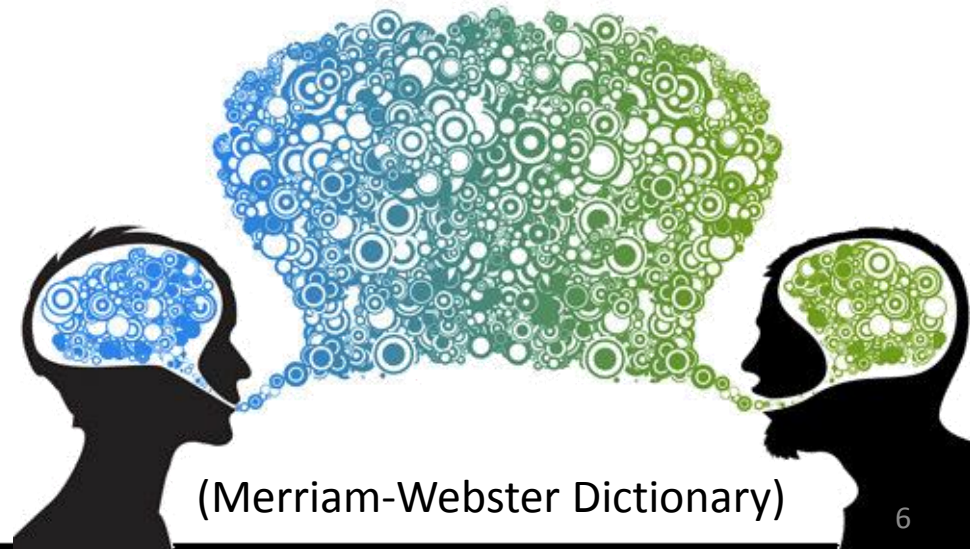
*~ Focus Group Member*



# How is it different from...

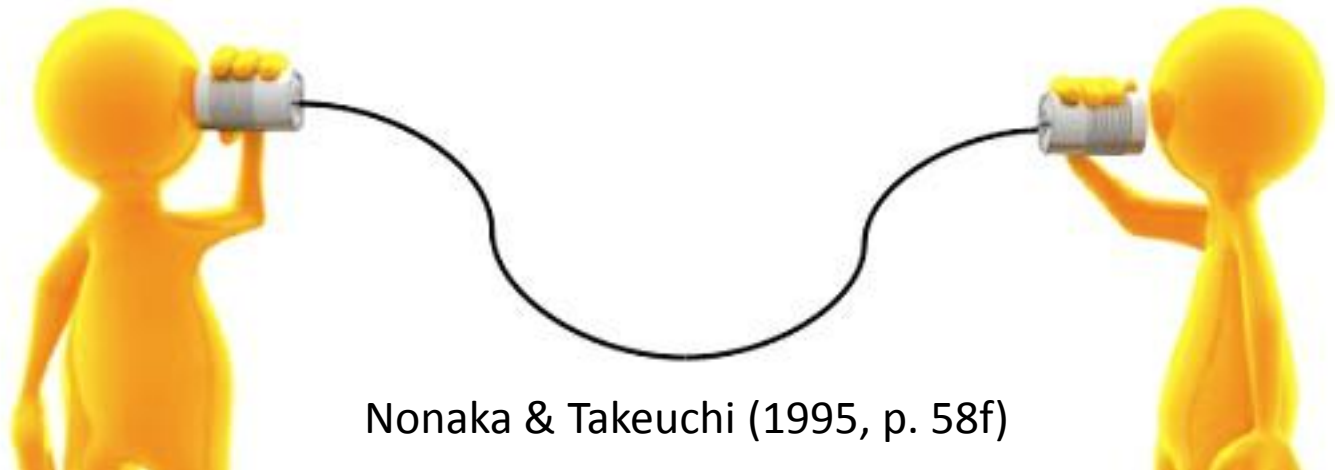
- **Communication**

- “the act or process of using words, sounds, signs, or behaviors to express or **exchange information or to express** your ideas, thoughts, feelings, etc., **to someone else**”



# How is it different from...

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



Nonaka & Takeuchi (1995, p. 58f)



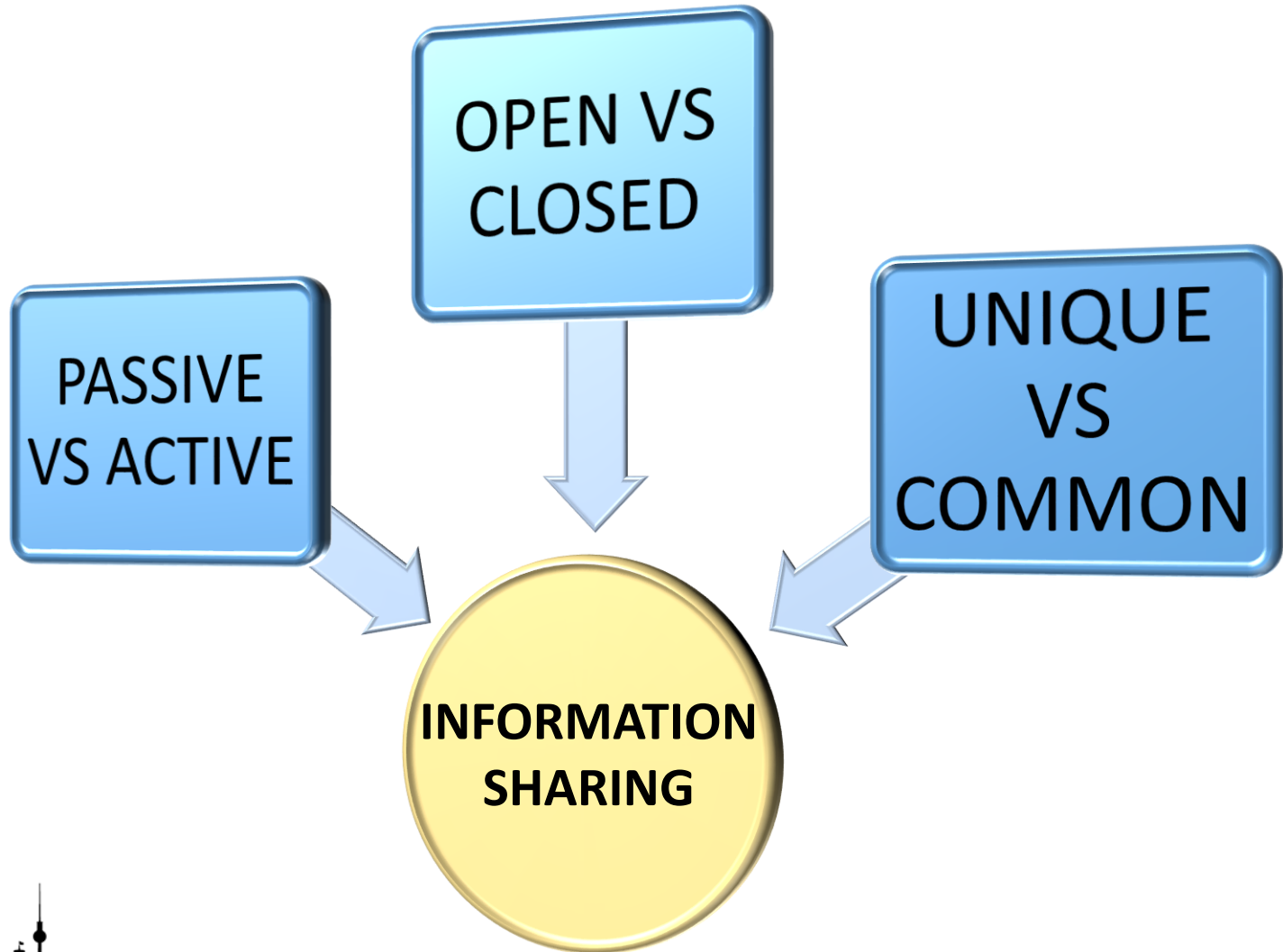
# Why Information Sharing is Important

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





# How does it work?



# Interpersonal Information Sharing: Passive vs. Active

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



# Passive or Active?

“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.”



# Socio-emotional Information Sharing: Open vs. Closed

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



# Open or Closed?

“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.”



# Task-related Information Sharing: Unique vs. Common

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



# Unique or Common?

“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.”



# Levels of Information Sharing

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

# Differences Across Levels

- **Within Teams**

- *Common* backgrounds and working norms
- More *frequent* contact

- **Between Teams**

- *Different* backgrounds and working norms
- *Variable* POCs, but working towards a *shared goal*

- **External**

- *Different* backgrounds and working norms
- *Variable* contact, with potentially *different goals*



# Identify the Level

“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.”



# 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

# How Information Sharing Works

- Helps establish **knowledge networks**
  - Social relationships that support (or limit) the acquisition, transfer, and creation of more knowledge
- Need to know:
  - **Who has what** information
  - **Who needs to know what** information





# How Information Sharing Works

"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."



# What Can Go Wrong?

- Information **overload**
  - Having more information than you can absorb
- Information **loss**
- **Wrong** information
- **Unavailable/missing** unique information
  - Missing cues during an incident
- Not knowing **who needs or has** the information
  - Or who should receive information



# What Else Can Go Wrong?

- **Late/delayed** information
- **Misclassified** information
- Knowledge **hiding**
  - Deliberate withholding of knowledge requested by others
  - Driven by individual motivations / goals
  - **Classification of incidents** can impact information sharing



# 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



# What Inhibits Information Sharing?

- Within the **Organizational** level
  - Hierarchical structure
  - Overly restricting rules
  - Socio-cultural barriers
  - Climate



# How to Develop Effective Information Sharing

## Two Methods

- Enhance task-related processes
- Consider team characteristics





# How to Develop Effective Information Sharing: **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)



# How to Develop Effective Information Sharing: **Strategies**

## Consider Team Characteristics

- Establish climates of trust and learning
  - Consider locations of team members\*
  - Use After-Action-Reviews
- Clearly define team roles
  - Create a knowledge catalogue
- Have a designated “boundary spanner” to share information with other teams
- Promote unique information sharing



# Let's Share Information!

## Discussion Questions:

- In your work, what type of information do you normally share/receive?
- How do you determine what types of information to share? What makes information relevant? How do you know what information others might be interested in or need?
- In what format do you share information? Why do you choose that format?
- Are there any types of information you do not share? Why? What would lead you to share that information?



# Thank you!

QUESTIONS OR COMMENTS:

KRISTIN REPCHICK, M.A.  
[KREPCHIC@GMU.EDU](mailto:KREPCHIC@GMU.EDU)

LAURA FLETCHER  
[LFLETCH5@GMU.EDU](mailto:LFLETCH5@GMU.EDU)

JULIE STEINKE, PH.D.  
[JSTEINKE@GMU.EDU](mailto:JSTEINKE@GMU.EDU)