
# International Capacity Building: Improving Cooperation and Information Sharing

Cybersecurity Workshop

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

# Document Markings



This material is based upon work funded and supported by the Department of State under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.



DM21-0132

# Introduction

- In an interconnected world, connecting with peers to learn and improve is more important than ever.
- Information Sharing is an critical in a number of areas: threats information, vulnerabilities, and incident response, as well as sharing best practices and cooperating in other areas.
- There are many resources, regionally and internationally, for cybersecurity leaders and managers to use to improve sharing.

# Agenda

- Why do we share?
- What makes sharing difficult?
- How can we do better?
- Summary
- If You Want to Know More

# Why should Incident Responders Share Information?

# Definition and Background

- **Sharing information** (such as incident information or other cybersecurity data) is an important part of working together, but there are other ways to connect, such as sharing best practices, sharing lessons learned, or working together to reduce other burdens.
  - **Connecting** is the process of joining or linking two or more things together, for the purpose of improving cooperation, communications, and sharing.

* Incident management teams need to connect with others in the security community about threat and other information found during the course of their investigations and research.

# Why Share for Cybersecurity?

- Gain awareness of threats that other organizations are experiencing.
- Learn about threats before (or after) they hit you or others.
- Help other organizations prevent threats that have affected you.
- Discover incidents you didn’t know about.
- Help others discover activity they didn’t know about.
- Improve your understanding of adversaries.
- Improve stability and security on the Internet by identifying, monitoring, taking down malicious sites, and discouraging ‘bad behavior.’
- Make it more challenging/costly for adversaries to conduct attacks.
- Agree upon shared norms etc.

# Why Connect with other Smart Cities? Desired Cybersecurity Outcomes

Security cannot be achieve in a vacuum – adversaries work across international borders, and apply lessons learned in one attack to the next. Smart City defenders and incident responders must do the same.

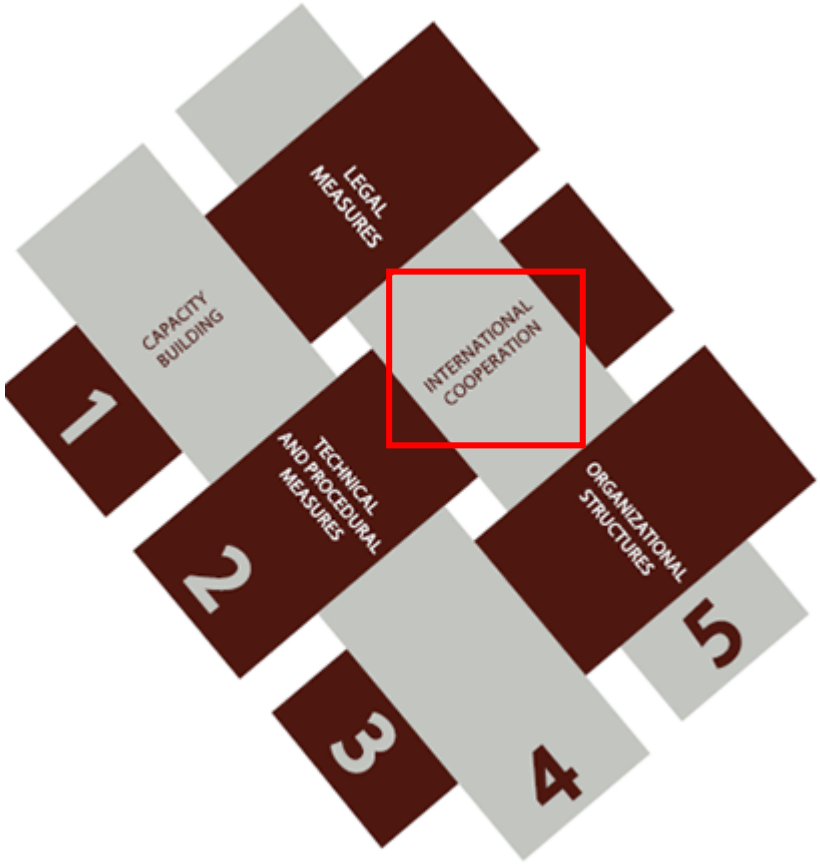
For example, according to NIST Publication 800-150, information sharing can result in improvements in the following areas:

- Shared situational awareness
- Improved security posture
- Knowledge maturation
- Greater defensive agility

Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

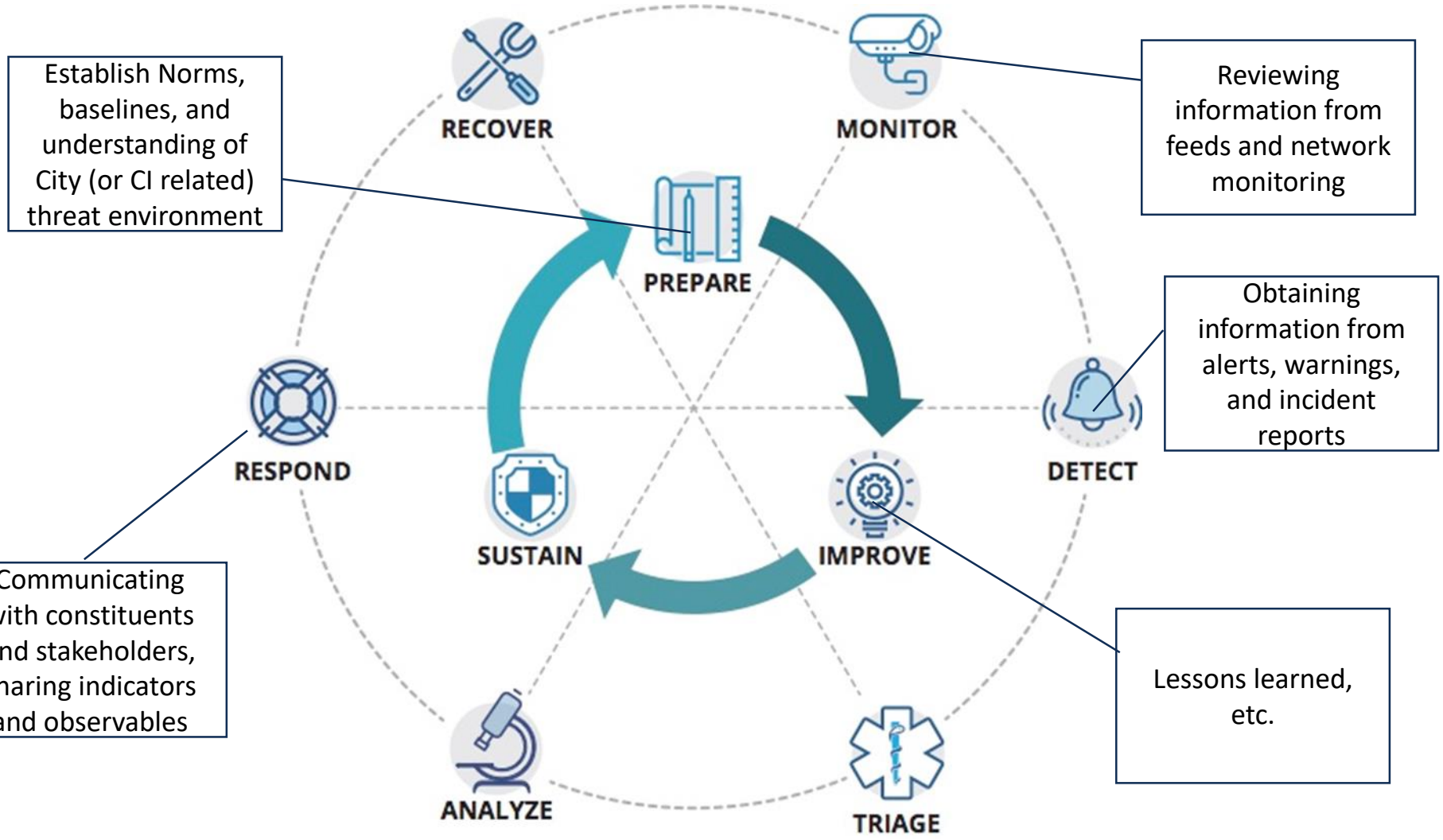
# Why Connect on Cybersecurity?

- **ITU Global Cybersecurity Agenda (GCA)**
  - "A framework for **international cooperation** aimed at enhancing confidence and security in the information society. The GCA is designed for cooperation and efficiency, encouraging **collaboration with and between all relevant partners** and building on existing initiatives to avoid duplicating efforts."




Source: https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

# The Incident Management Lifecycle – Opportunities to Connect and Cooperate




Establish Norms, baselines, and understanding of City (or CI related) threat environment

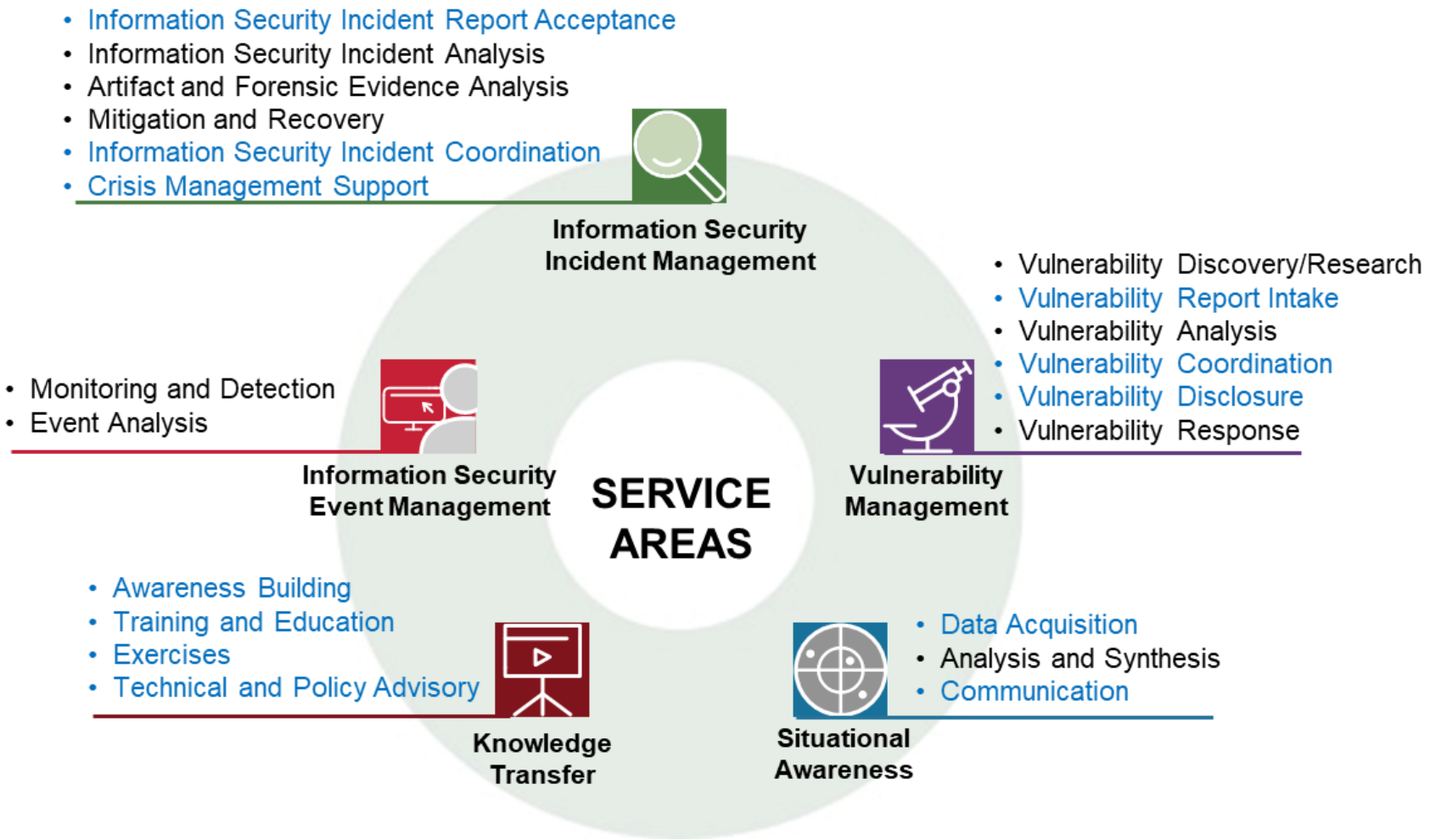
Reviewing information from feeds and network monitoring

Obtaining information from alerts, warnings, and incident reports

Communicating with constituents and stakeholders, sharing indicators and observables

Lessons learned, etc.

# Services Framework Including Communication & Sharing Activities




Source: https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

# Sharing Information and Cooperating on Cybersecurity – Internationally

International cybersecurity information sharing is the act of exchanging cybersecurity-related information, including IOCs, threat intelligence, vulnerability reports, and analyses with other cybersecurity and incident response teams (often CSIRTs or SOCs) in *other parts of the world*, often in areas with little geographic link.

Key Questions:

- How should information be shared?
- How to identify international peers for sharing?
- What information should be shared, and how?
- What challenges exist to establishing a mutually beneficial sharing regime?

# Connecting and Cooperating on Cybersecurity - Regionally

Regional cybersecurity cooperation is the act of exchanging cybersecurity-related information, best practices, lessons learned, and other tradecraft with other cybersecurity and incident response teams (often CSIRTs or SOCs) in a *common geographic area*.

Key Questions:

- How should information be shared?
- How to identify regional peers for cooperation?
- What should be shared, and how?
- What challenges exist to establishing a mutually beneficial sharing regime?

# Benefits of Connecting Regionally

- Knowledge transfer of common and regional-based threats
  - Similar threat surface or threat environment
- Encouragement of capacity building and awareness
- Cybersecurity and incident response community-building
- Transmission of best practices
- Common challenges and solutions

# Why Sharing Information is Difficult

# Challenges to Cooperation

- Overcoming distrust
- Member state or regional politics
- Diversity of members
- Determining shared value/vision
- Legal and regulatory requirements
- Lack of common taxonomy
- Technical barriers
- Lack of already established (internal) standardization and cooperation structures
- Governance/organizational issues

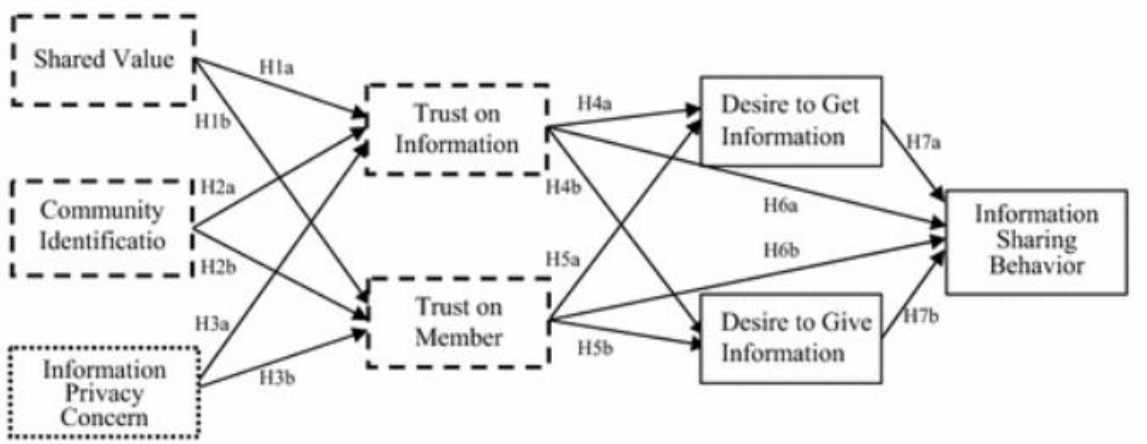
# Challenges – Trust

Sources of Distrust:

- Capability gaps
- Political issues
- Lack of communication

Sources of Trust:

- Face-to-face interaction (meetings, exercises, etc.)
- Well-established communications channels
- Clear policies and agreements




Source: https://link.springer.com/article/10.1007/s10257-015-0279-2

# Challenges – Politics

- Member state or regional political disagreements
- Political pressure (government or parent organizations)
- *However…*
  - Cybersecurity and threat actors transcend borders and politics.
  - Regional cooperation in the cybersecurity field can lead others in the diplomacy field.

# Challenges – Diverse Stakeholders

Includes diversity of:

- Capabilities/services
  - How can you manage the value-add for teams with varying capabilities and service offerings?
- Maturity levels
  - How do you manage the value-add for teams spanning a wide array of maturity levels?
- Sectors
  - If teams from multiple sectors are members of a single information sharing body, how do you ensure the information is relevant and actionable for all?

# Challenges – Shared Values and Vision

Individual entities often impart their vision and values onto a community, but often a community's vison and values are imparted upon the individual entity.

- How do communities agree on a shared set of values?
- How can entities retain their own identity while being a part of a community?
- Does information sharing reflect community values or individual values?
- Are there legal or regulatory differences between countries? Regional blocs (EU, ASEAN, etc.)?

# Legal Considerations – sharing information across jurisdictions

In the US, the 2015 Cybersecurity Information Sharing Act:

- US Government will publish best practices
- Federal government outlines rules for disclosure, retention, use, etc. of data
- Provides legal mechanisms (including liability protection) for organizations to share information with federal government vis DHS
- Provides privacy protections by requiring entities to remove identified PII from any information shared with federal government.

*"Authority for cybersecurity information sharing between and among the private sector; state, local, tribal, and territorial governments; and the Federal Government"*

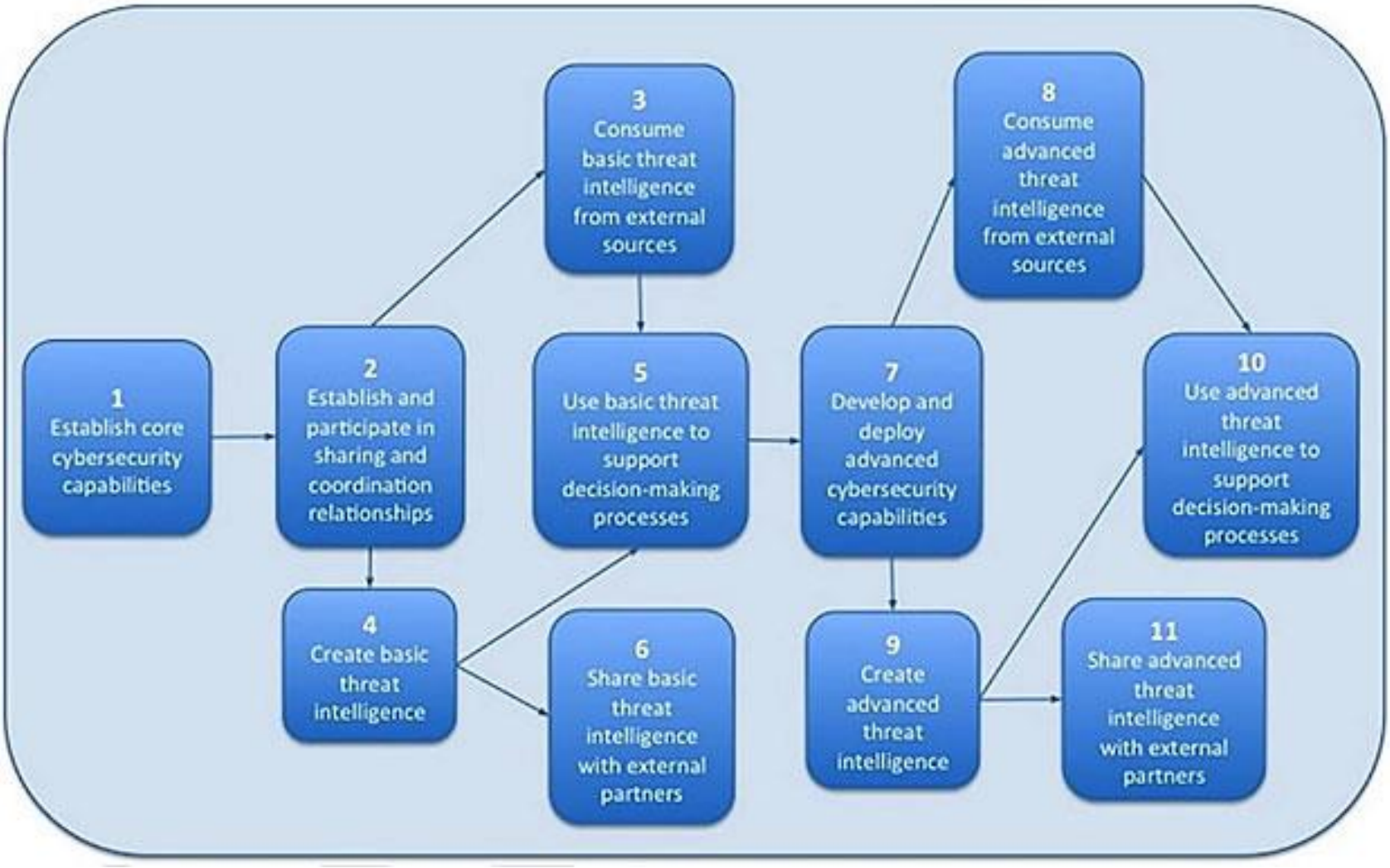
Source: https://www.cisa.gov/sites/default/files/publications/Non-Federal%20Entity%20Sharing%20Guidance%20under%20the%20Cybersecurity%20Information%20Sharing%20Act%20of%202015_1.pdf

# How can we Achieve Information Sharing and Cooperation?

# When Establishing Relationships

- Define the goals and objectives of the relationship.
- Identify internally how you want to connect, and what will be shared (data vs best practices, etc.)
- Define the scope of activities.
- Establish common rules and boundaries.
- Join a community.
- Plan to provide ongoing support for activities.
- Build **Trust**!

# NIST Information Sharing Process



# Use a Framework

**NIST 800-150:2016**

It is widely used within and outside of the United States because NIST distributes all of its standards documents without charge.

NIST does not maintain an independent certification based on its body of standards.

**ISO 27010:2015**

ISO's main advantage in the context of standards is their broad applicability internationally.

ISO standards documents must be purchased.

ISO also maintains a certification mechanism using their primary information security standard (ISO 27001).

# International Organizations

## Forum of Incident Response and Security Teams (FIRST)


**FIRST Vision**

FIRST aspires to bring together incident response and security teams from every country across the world to ensure a safe internet for all.

*Effective response is a global task, mirroring the global nature of the internet. Based on a peer to peer network governance model, Computer Security Incident Response Teams (CSIRTs), Product Security Incident Response Teams (PSIRTs) and independent security researchers work together to limit the damage of security incidents. This requires a high level of trust; the fuel our members run on. FIRST fosters trust building among members through a variety of activities. Incidents are not confined to one cultural or political corner of the internet, nor do they respect borders or boundaries. FIRST thus promotes inclusiveness, inviting membership from all geographic and cultural regions.*

Source: https://www.first.org/about/mission

# FIRST Mission

**Global Coordination - You can always find the team and information you need.**

*FIRST provides platforms, means and tools for incident responders to always find the right partner and to collaborate efficiently. This implies that FIRST's reach is global. We aspire to have members from every country and culture.*

**Global Language - Incident responders around the world speak the same language and understand each other's intents and methods.**

*During an incident it is important that people have a common understanding and enough maturity to react in a fast and efficient manner. FIRST supports teams through training opportunities to grow and mature. FIRST also supports initiatives to develop common means of data transfer to enable machine to machine communication.*

**Policy and Governance - Make sure others understand what we do, and enable us rather than limit us.**

*FIRST members do not work in isolation, but are part of a larger system. FIRST engages with relevant stakeholders, in technical and non-technical communities, to ensure teams can work in an environment that is conducive to their goals.*

Source: https://www.first.org/about/mission

# Summary

- Cybersecurity teams and incident responders face unique and growing threats.
- One way to combat these threats is by cooperating and connecting with other teams.
- Because teams often face similar threats, they can learn from each other, share valuable data and experience, and leverage resources more efficiently.
- There are many ways to share:
  - Regionally
  - Internationally
  - Multilateral or Bilateral

# If You Want to Know More

NIST Information Sharing: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

Trust: https://link.springer.com/article/10.1007/s10257-015-0279-2

CSIRTs and Politics/Diplomacy: https://onlinelibrary.wiley.com/doi/pdf/10.1111/1758-5899.12625

# Questions