Coordinated Incident Handling

Aug. 20, 2014

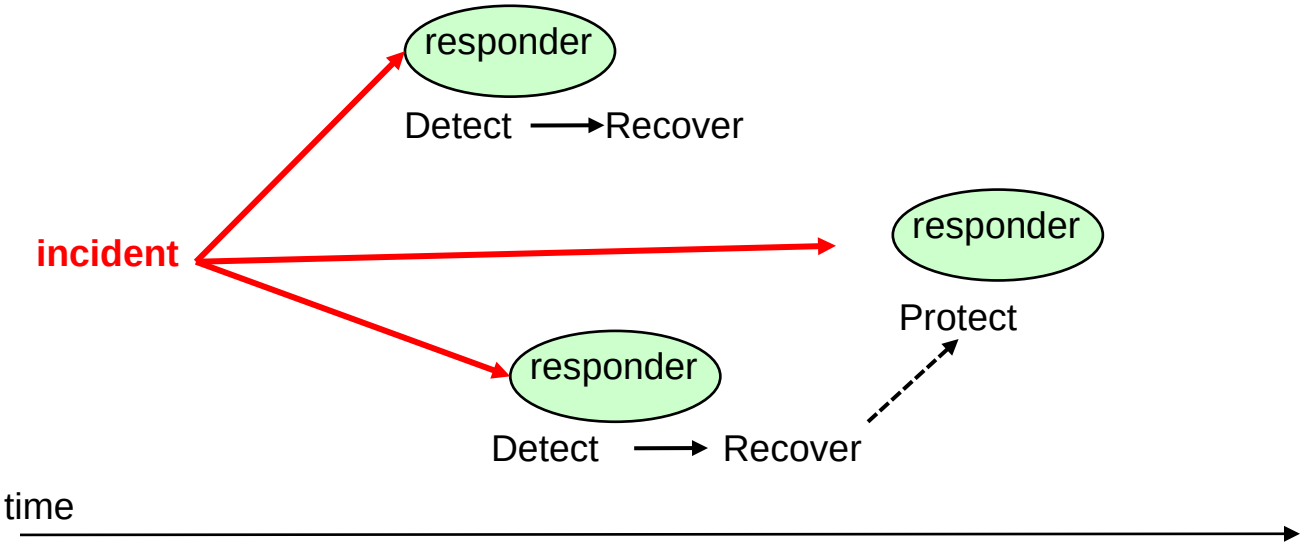
Lee Badger
David Waltermire
Christopher Johnson
NIST

Note: Any mention of a vendor or product is not an endorsement or recommendation.

Nutshell View

A Computer Security Incident = A **violation** or **imminent threat of violation** of computer security policies, acceptable use policies, or standard security practices.

Source: SP 800-61



1. We are developing **SP800-150**, providing guidance on safe, effective information sharing.
2. This will supplement existing NIST guidance on incident handling, SP 800-61.
3. This will fit into the context of the Cybersecurity Framework developed under the authority of Executive Order 13636 on the protection of critical infrastructure.

Benefits for Coordination and Sharing

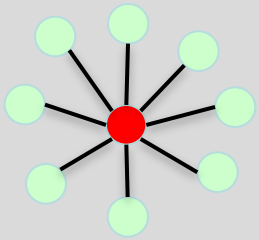
- Shared Situational Awareness
- Enhanced Threat Understanding
- Knowledge Maturation
- Reduced Cost
- Greater Defense Agility
  - Evolving TTPs
- Improved Decision-making
- Efficient Handling of Information Requests
- Rapid Notification

Challenges for Coordination and Sharing

- Legal and Organizational Restrictions
- Risk of Disclosure
- Preserving Anonymity
- Collecting Information
- Determining Adversary Motives
- Interoperability
- Classification of Information
- Organizational Maturity
- **Establishing Trust**

Information Sharing Architectures

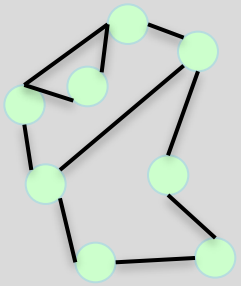
Centralized



Coordinating team can filter-anonymize communications

- Reduce risk (trust)
- Improve service
- Implement policies
- Single point of failure

Peer-to-peer

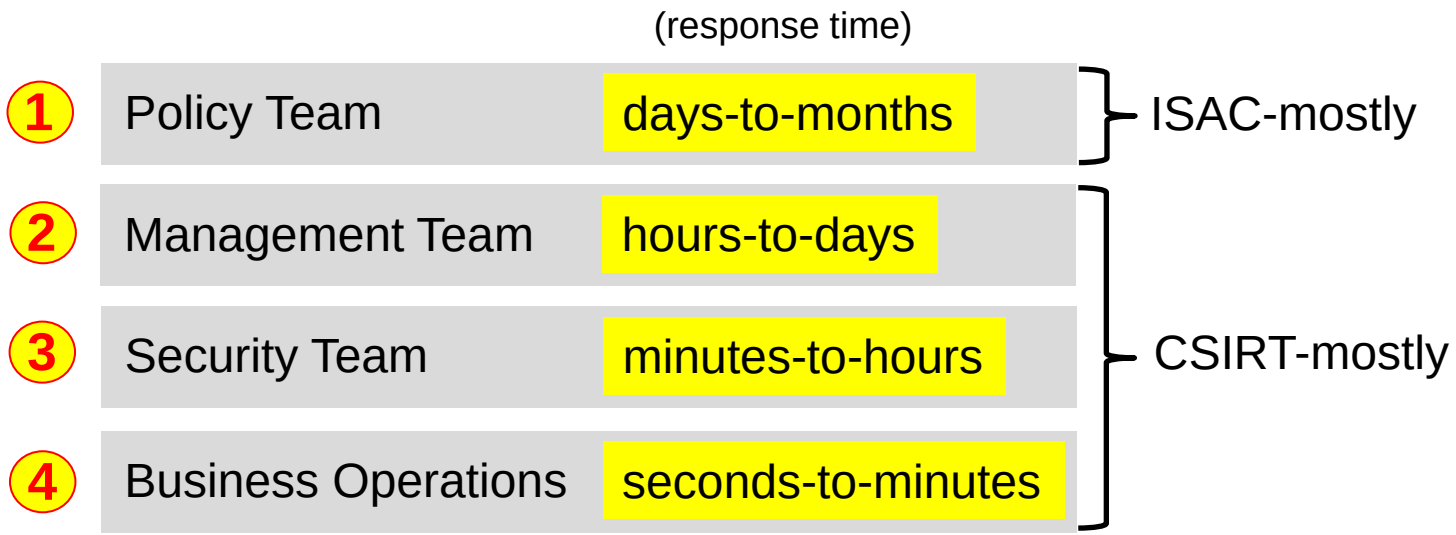


May not have a coordinating team

- Resilient
- Store-and-forward
  - Sharing along the path
- Latency may be high
- Quick to form

A Few Information Sharing Communities (a note about timing)

ISAC - Information Sharing and Analysis Center.
CSIRT - Computer Security Incident Response Team.



SP800-150 will provide guidance about all four response tempos, but our focus will be on the CSIRT levels.

ISACs

95% wired coms*
Communications

100% bulk pwr gens*
Electric Sector

Emergency Services

99% banks, CUs*
Financial Services

Health Services

85% routers*
Information Technology

Maritime

Multistate

Nuclear

90% riders*
Public Transit

Real Estate

Research & Education

Supply Chain

95% rail*
Surface Transportation

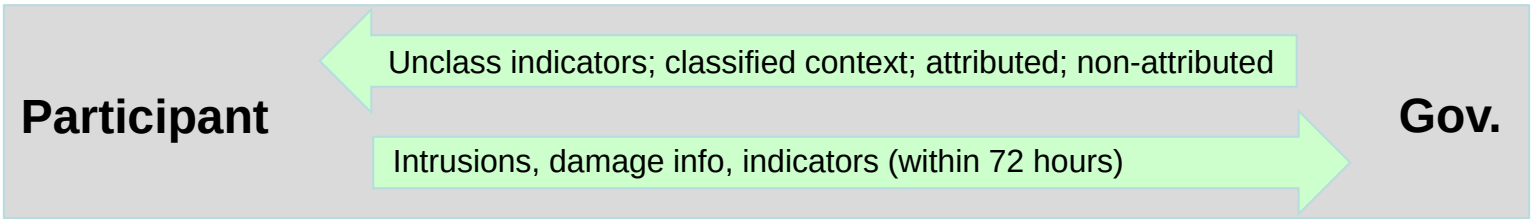
65% consumers*
Water

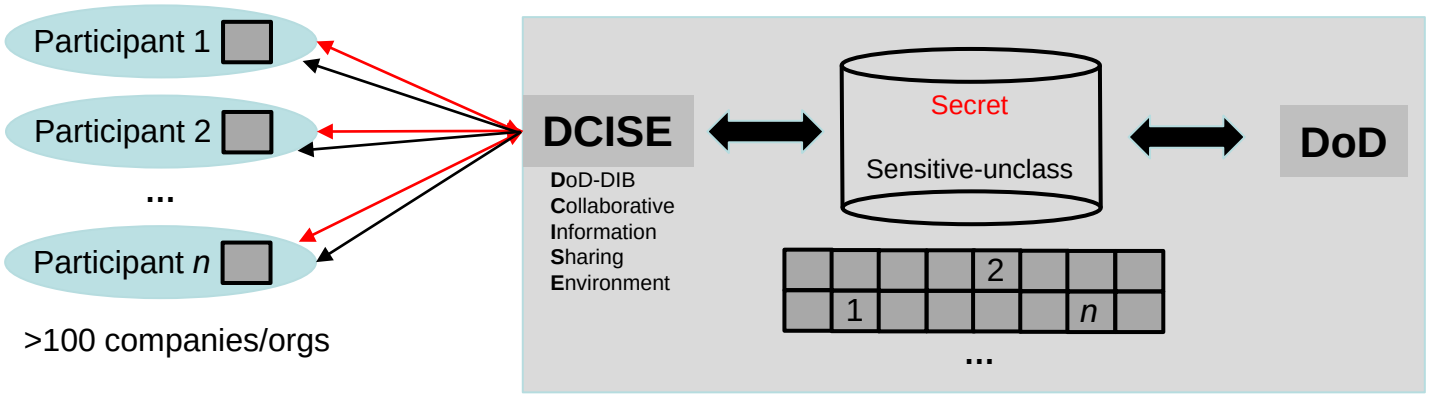
"an ISAC is a trusted, sector specific entity which … collects, analyzes, and disseminates alerts and incident reports to … provide analytical support to government and other ISACs" *

1. Public/private sector security cooperation.
2. Daily info exchange
3. Weekly meetings.
4. Threat Response & Reporting Guidelines

Credit: http://www.isaccouncil.org
* http://www.isaccouncil.org/images/ISAC_Role_in_CIP.pdf (red = coverage, or "reach")

DiBNET





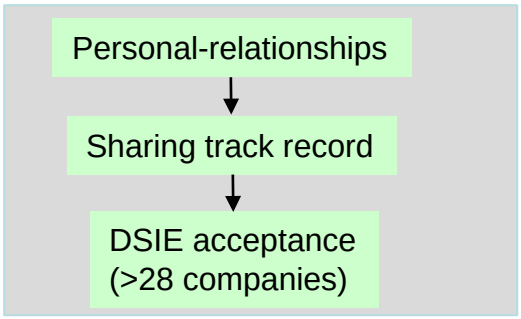
- Voluntary sharing; public and private
- Protect sensitive but unclassified info
- Eligibility: >= Secret Facility Security Clearance; COMSEC, DoD-approved certificates
- Sign the Framework Agreement; Perform legal review
- Clear responsibilities enumerated in advance
- **Trust.**

Ref: Federal Register Vol 77, No. 92.

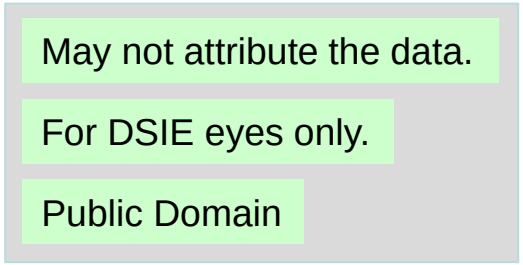
Non-attributed: →
Attributed: →

Defense Security Information Exchange (DSIE)

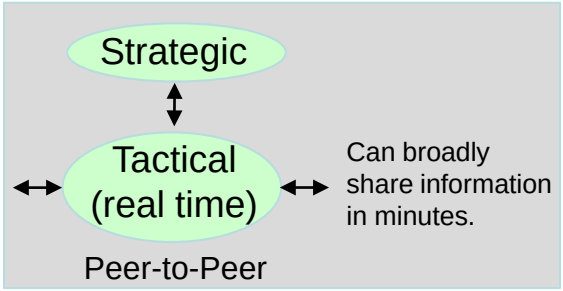
Trust Model



Sharing Levels



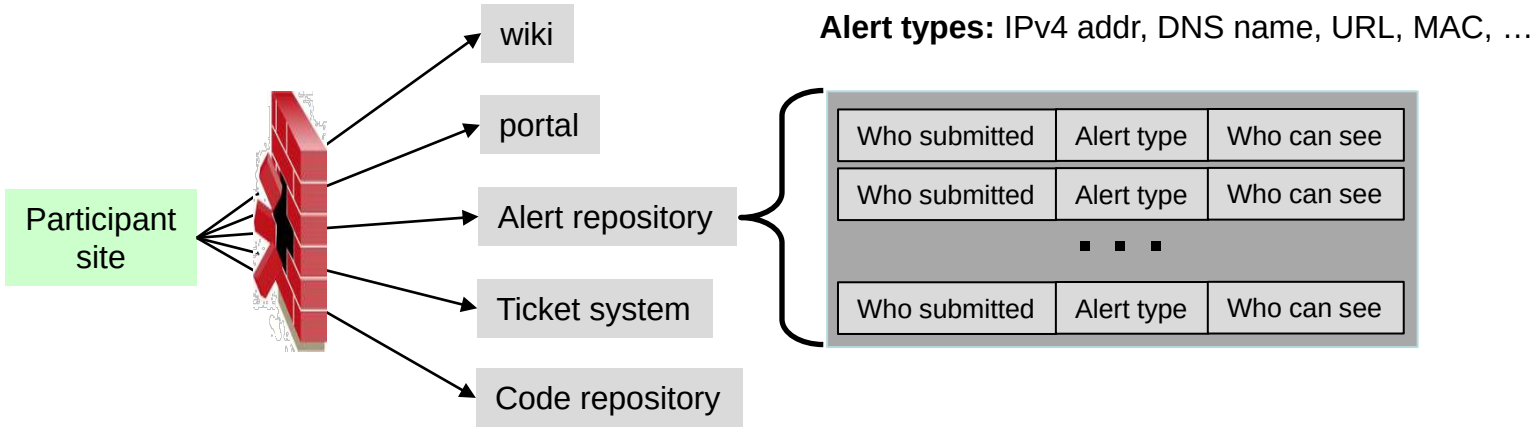
Committee Structure



- Mission: protect DoD Critical Infrastructure and Key Resources (CIKR)
- Eligibility: NDA; >= Secret clearance
- Voluntary
- Bi-monthly meetings at non-attributionable level
- Goal: eventually partner with DIB regarding cyber CIKR

Source: http://www.whitehouse.gov/files/documents/cyber/Defense%20Security%20Information%20Exchange%20-%20DSIE%20summary%20-%20William%20Ennis.pdf

Cyber Fed Model



- ~20 Gov. agencies, research, educational, and business organizations
- Requires a Memorandum of Understanding (MOU)
- Sharing among trusted entities
- An alert distribution system (5 minute typical distribution time)
- An alert can suggest an action (e.g., “block”)
- Participant sites grouped into federations
  - Facilitates group-based distribution, use public/private keys

Credit: http://web.anl.gov/it/cfm/index.html

More Sources of Insight

We have held general conversations with practitioners.

Jeff Carpenter (former CERT CC)
Ben Miller (NERC)
Pat Dempsey (DCISE)
Anton Chuvakin (Gartner)
Mike Murray (CERT CC)
Dr. Johannes Ulrich (SANS Institute)
Garrett Schubert (CIRT Team-Lead at EMC)
Matthew Schuster (Mass Insight & ASTC)
James Caulfield (Federal Reserve)
Bob Guay (Manager, Information Security, Biogen)
Chris Sullivan (Vice President, Product Planning, Courion)
Jon Baker (MITRE)

Organizational maturity varies a **lot**.

Estimating both trust and report-quality is currently subjective: have to work with this.

An indicator file reveals what we can see.

A few observations (not consensus) on the topic of indicators:

SIMPLE facilitates sharing;
COMPLEX impedes sharing.
many-screens == bad
cheap-tools == good

DCISE: 80+ element xml schema and ZERO adoption, even by the authors.

A decline of average-maturity is natural as a community grows.

Expanded CSV is practical:
(indicator, type, role, attack-phase, comments).
A taxonomy regarding roles and types is defined but closely held.

HARD PROBLEM: establishing trust relationships in a circle of sharing.

NO HANDCUFFS!

Establishing Sharing Relationships

- Defining Goals, Objectives, and Scope of Information Sharing
  - Mission specifics; resources; approvals;
- Conducting an Information Inventory
- Establishing Information Sharing Rules
  - Sources; sensitivity; restrictions
- Joining a Sharing Community
  - Info actionable; mechanisms; NDAs, etc.
- Supporting an Information Sharing Capability – resources; proactive measures

Participating in Sharing Relationships

- Engaging in On-going Communication
- Implementing Access Control Policies for Shared Information (locally generated, received info (e.g., DHS TLP))
- Storing and Protecting Evidence
- Consuming and Responding to Alerts and Incident Reports (vulnerable? Mitigation-effective? Have skills? Costs?)
- Consuming and Analyzing Indicators (monitoring infr)
- Creating Written Records
- Performing Local Data Collection
- Producing and Publishing Indicators
- Producing and Publishing Incident Reports

Data Handling Considerations

- What types of data to collect, share?
- What types of data to retain; how long; how to track/protect?
- **Risk of sharing vs risks of not sharing?**

Sometimes defined in Framework Agreements, and in general guidance.

e.g., DiBNET

participant: within company
need-to-know
US citizens

government: restrict internal
use & disclosure

e.g., DSIE

May not attribute the data.

For DSIE eyes only.

Public Domain

e.g., Cyber Fed Model

Federations restrict distribution.

Indicators only (so far).

Who submitted / who can see.

e.g., US-CERT Traffic Light Protocol

Red: limit to specific exchange, meeting

Amber: limit to own org, with need to know.

Green: limit to peers & partner orgs, community

White: no restriction except copyright

A few Take-Aways

- Need to operate at time scales consistent with the information.
- Trust leverages personal connections, operational record, legal processes.
- Trust is paramount and hard to achieve fast, but preparation helps.
- Larger communities are harder to trust.
- Organizational abilities vary greatly.
- Clear responsibilities should be enumerated before sharing.
- Simplicity facilitates sharing.

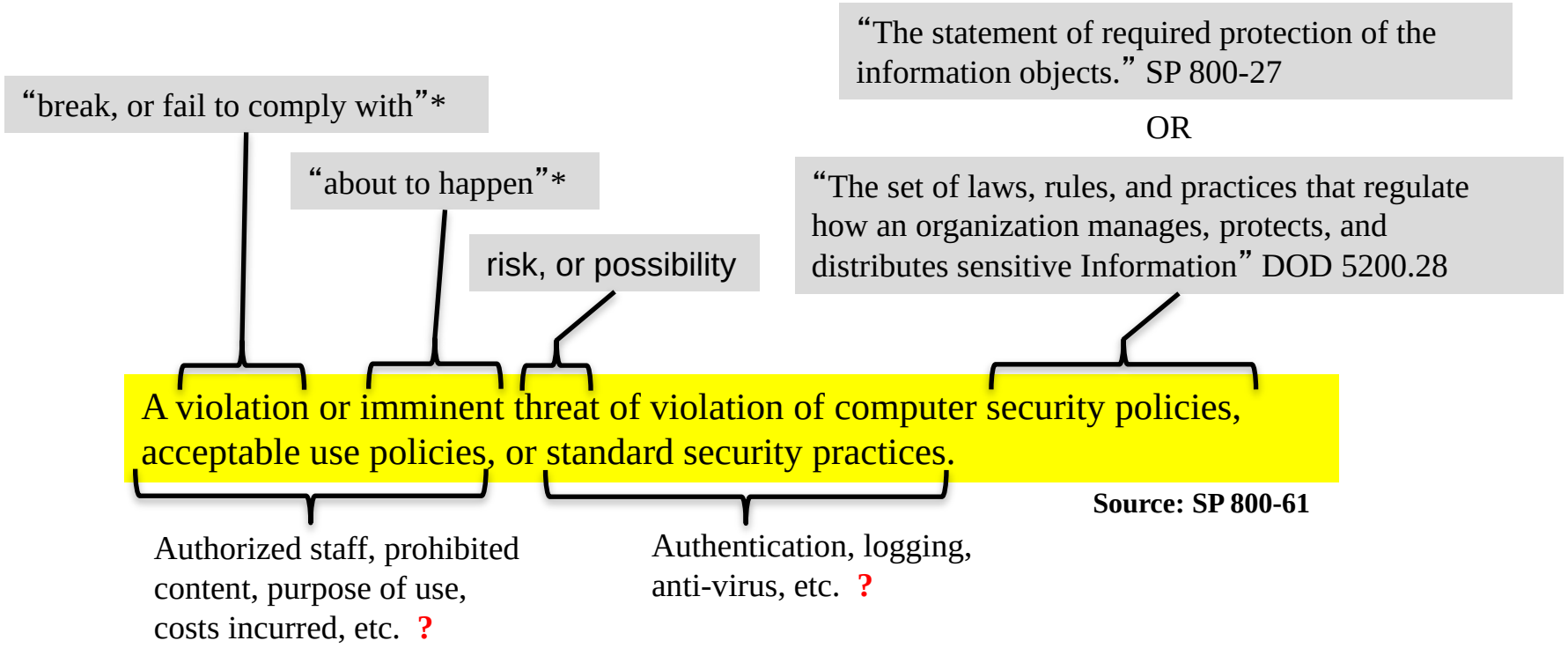
Status and Next Steps

- We are working on a draft of SP800-150.
- We hope to release a public draft in 1 or 2 months.

Contact: Lee Badger lee.badger@nist.gov
Christopher S. Johnson **christopher.johnson@nist.gov**
David Waltermire david.waltermire@nist.gov

Backup

Informal Definition of a Computer Security Incident



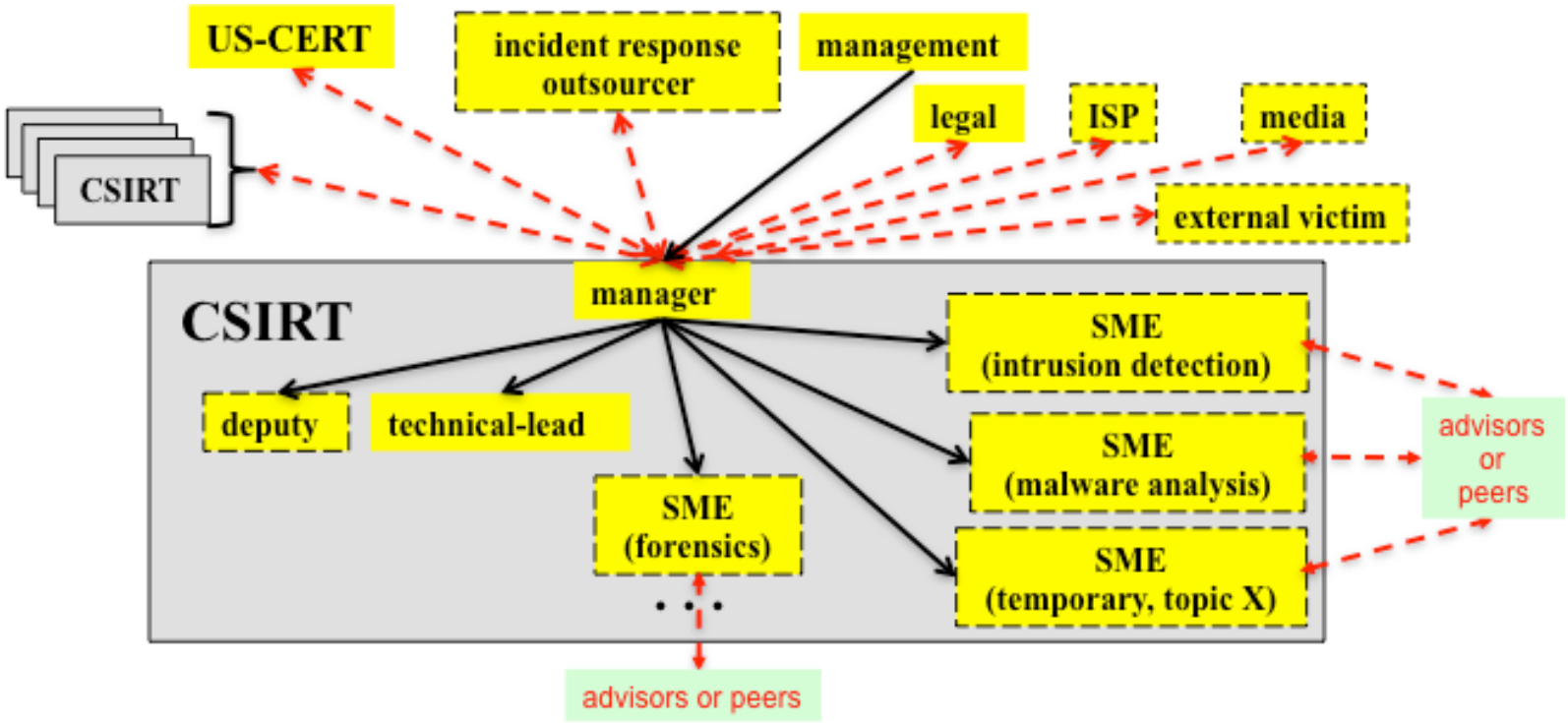
- Some ambiguity
- Includes MANY events
- Can't handle them all

Other, similar, definitions are in NISTIR 7298.
* Oxford dictionary

What is coordinated incident handling

- Communication and cooperation with external entities during an incident response
  - Two or more organizations
  - Exchanging information
  - Achieving common goals
    - Fast, effective incident response
  - Limiting exposures
    - Protecting sensitive information

Role Structure of a Computer Security Incident Response Team (CSIRT)

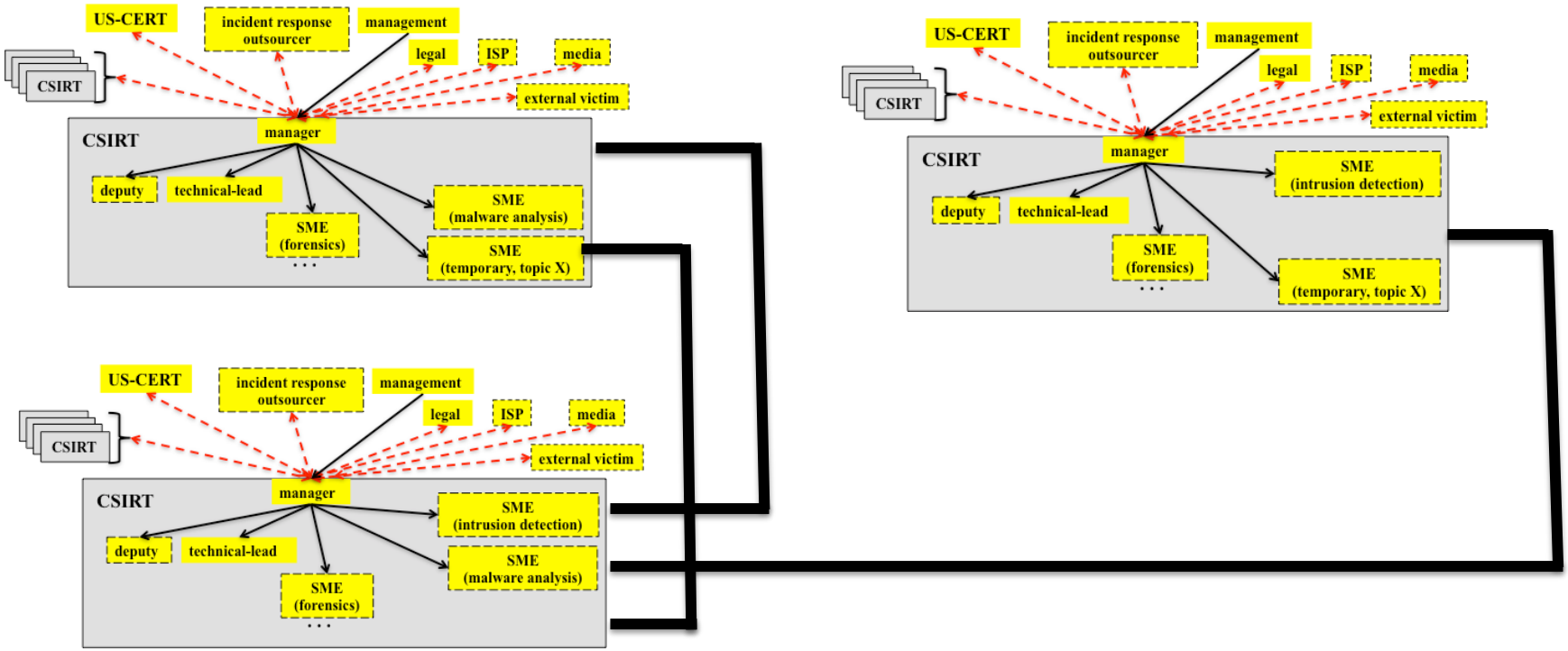


Legend:

optional:
authority:
communication:

- Operation brings together numerous professional skill sets.
- Manager authorizes SMEs to work with external advisors and peers.
- Communication follows skill sets and personal relationships.
  - Not necessarily a repeatable process

Notional Coordinated Role Structure of Computer Security Incident Response Teams



- Composed team can fill each others' gaps
- Some roles appear amenable to sharing (e.g., SMEs, ISP, US-CERT)
- Others, like management and legal, may need to exist for each participant

Legend:

optional:

authority:

communication:

Data Handling Considerations

Data handling rules derived from an **Information Lifecycle**:

- **Preparation**
  - Define data types: e.g., IP addresses, URLs, packets.
  - Identify exchange formats: e.g., email, structured documents.
  - Define markings: e.g., FOUO, company X proprietary, sensitivity markings.
  - Define sharing/tracking rules.
- **Collection**
  - A spectrum ranging from email cut/paste to manual forms to structured documents.
  - Choose information representations for collection.
- **Management & Processing**
  - Urgency, alerting, sensitivity, restrictions.
  - Storage, retention, error correction (e.g., erroneous sharing).
- **Sharing or Disclosure/Disbursement**
  - Authorities (management, legal, etc.) involved.
  - Develop frameworks.
  - Define chain-of-custody.
  - Do this in advance.
- **Retention & Disposition**
  - Time limits; National Archives and Records Administration (NARA) guidance vs longer retention to detect patient attackers.

Source: Information Lifecycle from DoD 8000.01

Understanding Organizational Capabilities

- Maintain a list of key contacts?
- How many staff involved in incident coordination?
- Provide monitoring/analysis/information to others?
  - or just consume it?
- Multiple communications mechanisms (net, phone, etc.)?
- Written response plan?
- Pre-approved response/sharing actions?
- Sensitive information labeled? (e.g., PII, proprietary)
- 24/7 availability of management?
- Documented incident resolution?
- Regular incident/coordination review meetings?
- Active skillsets: network sniffing, system administration, firewall administration, reverse engineering, malware analysis, …?
- Expertise person-based, or position-based?