GJØVIK UNIVERSITY COLLEGE

Security planning and Incident Management

Marie Moe, NSM/HiG

Gjøvik 03.03.14

AGENDA

Incident Response Planning

- *Incident response policy*
- *Incident response plan*
- *Forming a security incident response team*
- *Required skills and components*

Organizational models for CSIRTs

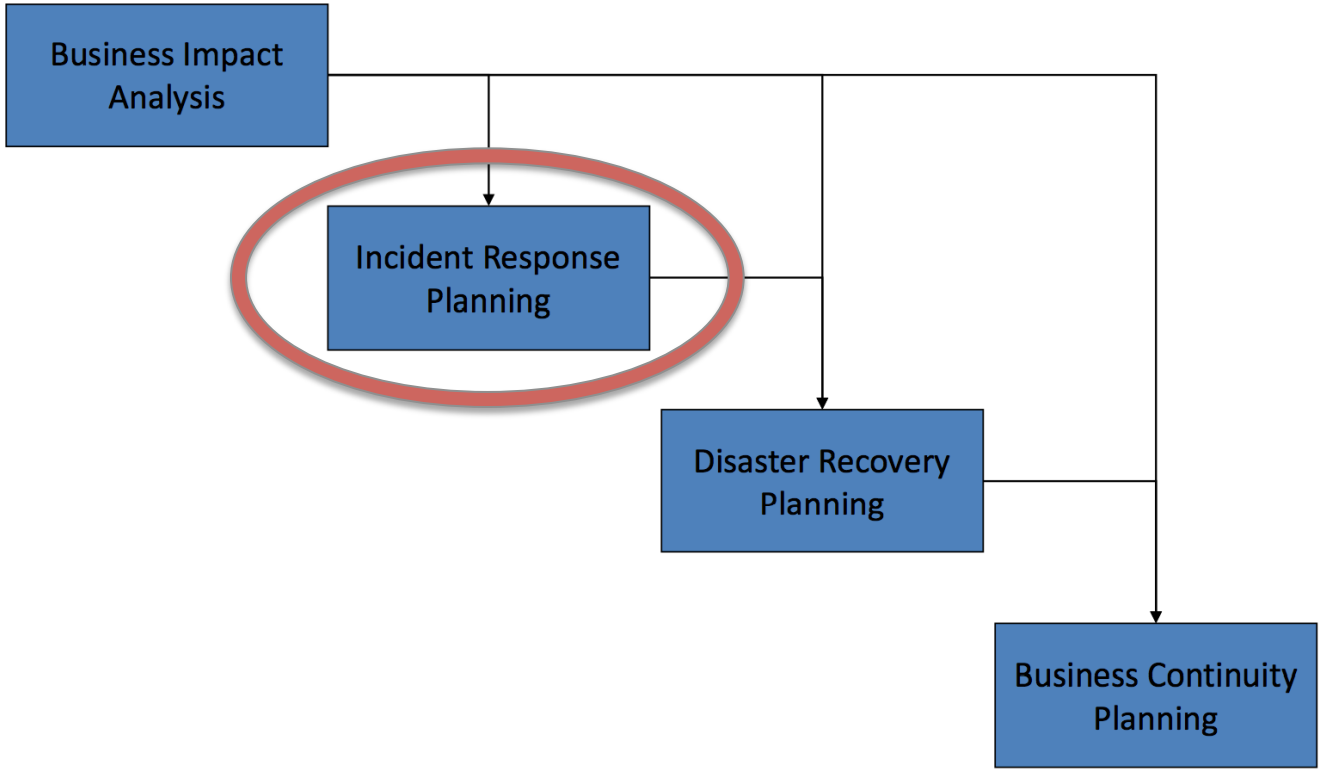
- *Establishing CSIRT capabilities*
- *Comparison of organizational models*
- *Operational issues*

“We frontload a lot of effort onto protecting things, but when a breach occurs we look round and ask ‘what do we do now?’ There’s no worse time to work out your response strategy than when you’re in the middle of responding to it.”

John Ellis, Enterprise Security Director at IT firm Akamai

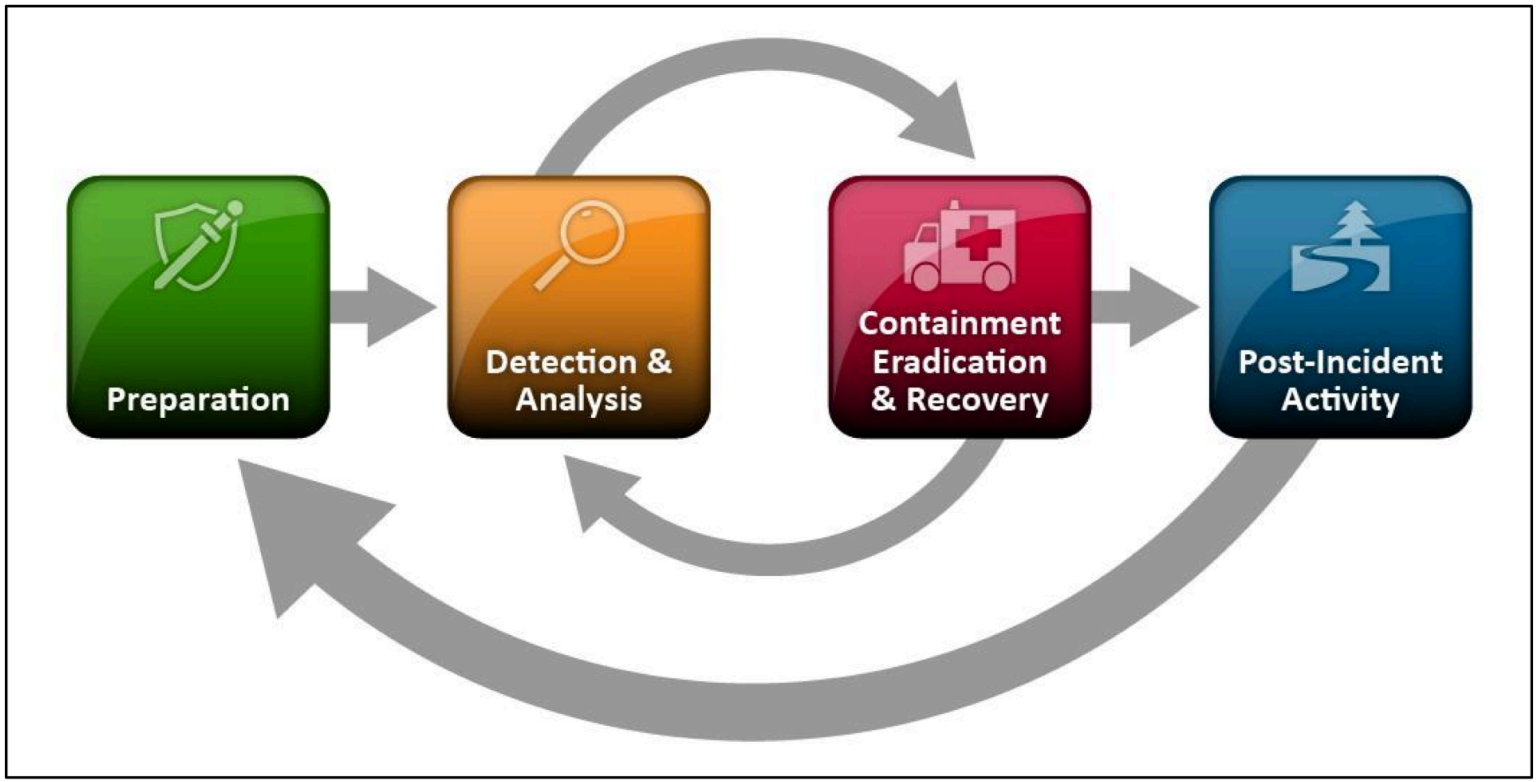
http://www.insurancebusinessonline.com.au/news/you-will-be-hacked--its-inevitable-says-cyber-security-expert-184625.aspx

COMPONENTS OF CONTINGENCY PLANNING



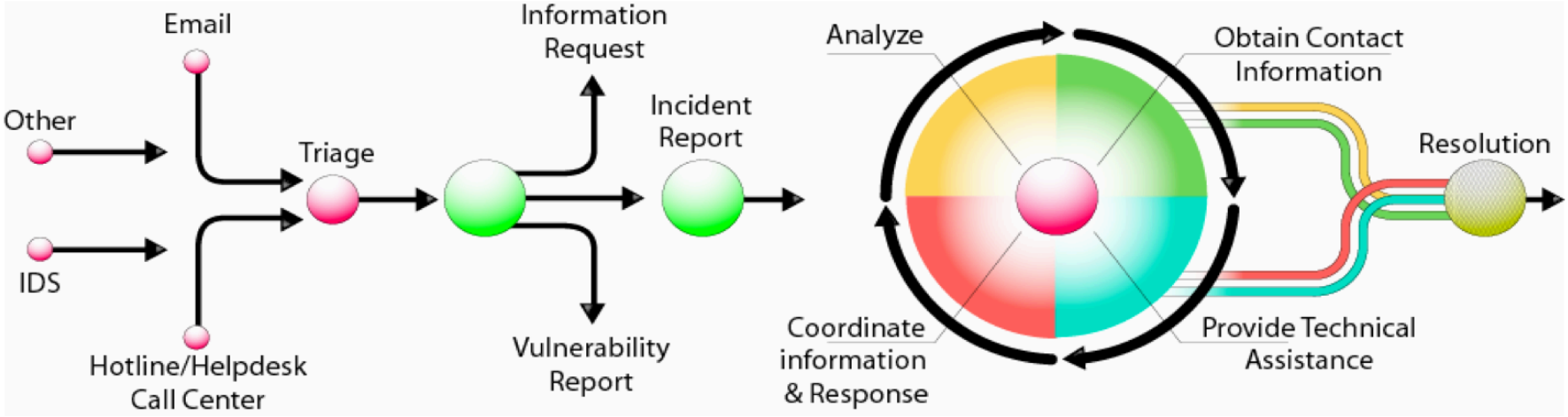
Whitman and Mattord 2007, p. 24-25

INCIDENT RESPONSE LIFE CYCLE (NIST)



NIST SP 800-61, Revision 2

INCIDENT HANDLING LIFE CYCLE (CERT/CC)



Handbook for Computer Incident Response Teams (CSIRTS)

THE IR PLANNING PROCESS

1. Form the IR planning committee
2. Develop IR planning policy
3. Integrate the BIA
4. Identify preventive controls
5. Organize the CSIRT
6. Create IR strategies and procedures
7. Develop IR plan
8. Ensure plan testing, training and exercises
9. Ensure plan maintenance

Whitman, Mattord and Green 2014, p. 133

FORMING THE IR PLANNING TEAM

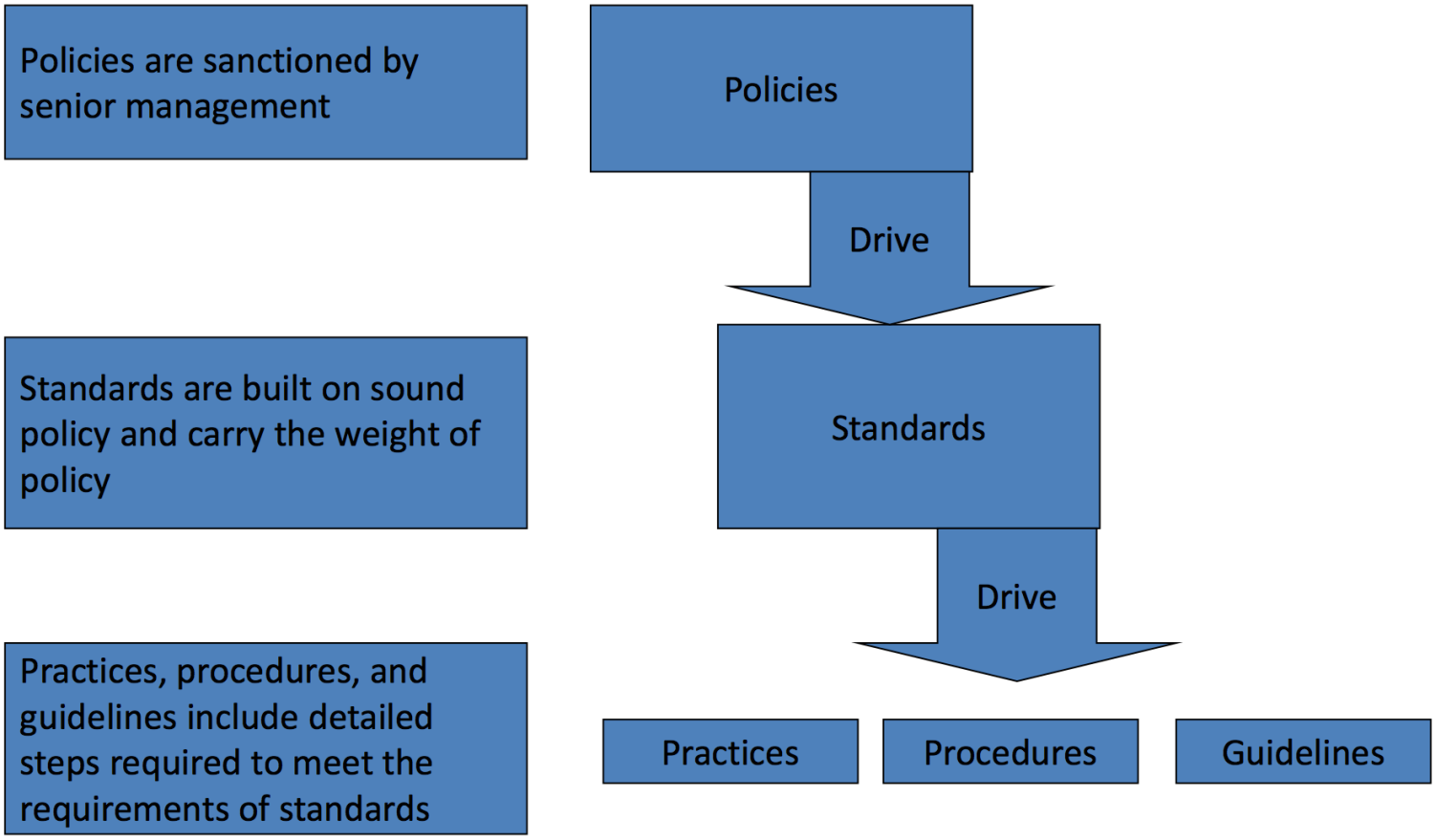
Has to be multi disciplinary

Relevant stakeholders should be represented

Typical members are:

- General management
- IT management
- InfoSec management
- Legal department
- Human Resources
- Public Relations

INCIDENT RESPONSE POLICY



Whitman and Mattord 2007, p. 30

INCIDENT RESPONSE POLICY ELEMENTS

- Purpose and objectives
- Scope
- Definition of information security incidents and their consequence within the context of the organization
- Organizational structure and delineation of roles, responsibilities and levels of authority
- Prioritization or severity ratings of incidents
- Performance measures
- Reporting and contact forms

Whitman, Mattord and Green 2014, p. 136

*A good **incident response policy** has to be:*

- Endorsed by management
- Clear
- Concise
- Necessary and sufficient
- Usable
- Implementable
- Enforceable

INCIDENT RESPONSE DEFINITION

Adverse event: *Unexpected activities that occur periodically.*

Incident: *An adverse event that affects information resources and/or assets causing actual damage or disruption.*

Incident response: *A set of procedures that commence when an incident is detected.*

Incident response procedures are **reactive measures** and are *not considered preventive controls.*

THE INCIDENT RESPONSE PLAN

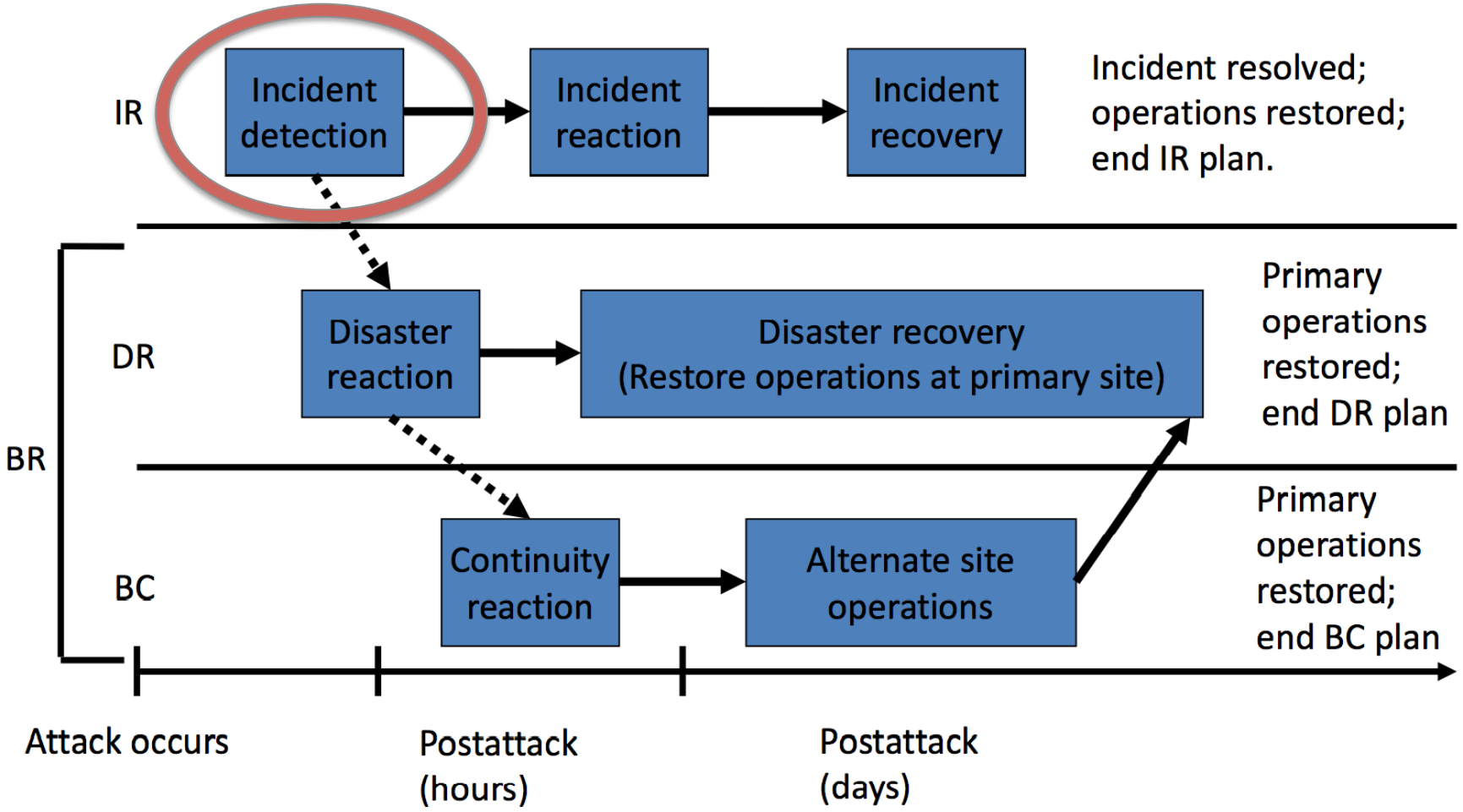
For *every potential attack scenario* the IR planning team creates an incident response plan

The IR plan contains three sets of incident handling processes:

- *During the incident*
- *After the incident*
- *Before the incident*

The IR plan includes the *trigger*, *notification method* and *response time*.

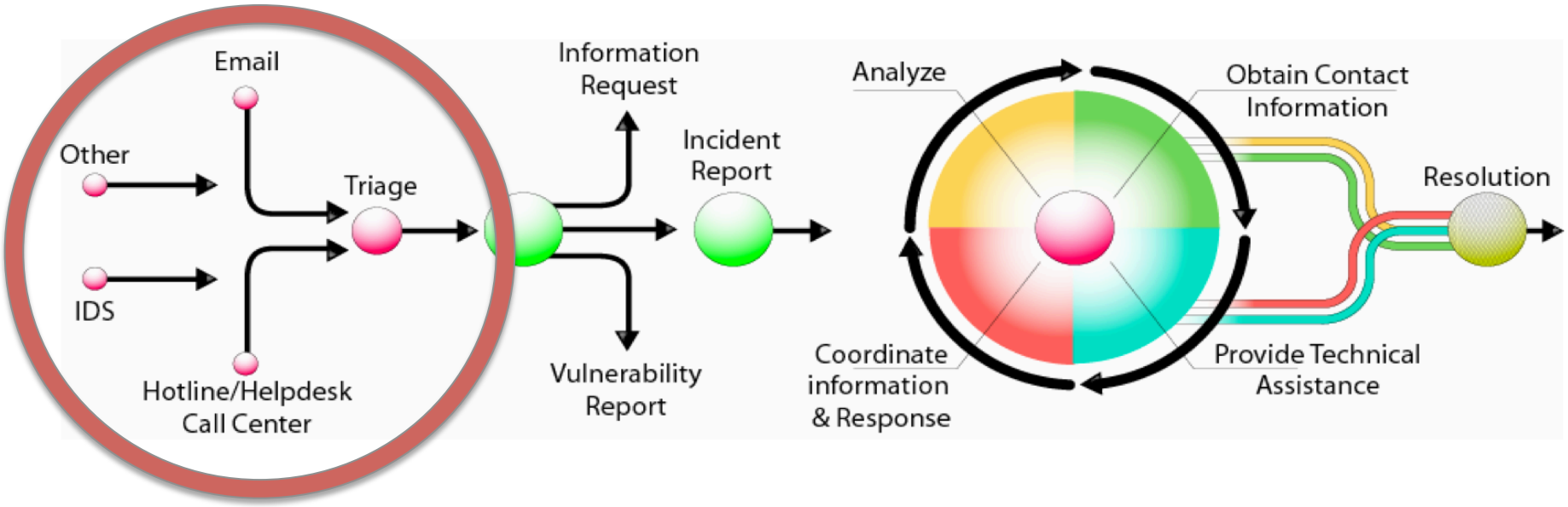
TIMELINE FOR CONTINGENCY PLAN EXECUTION



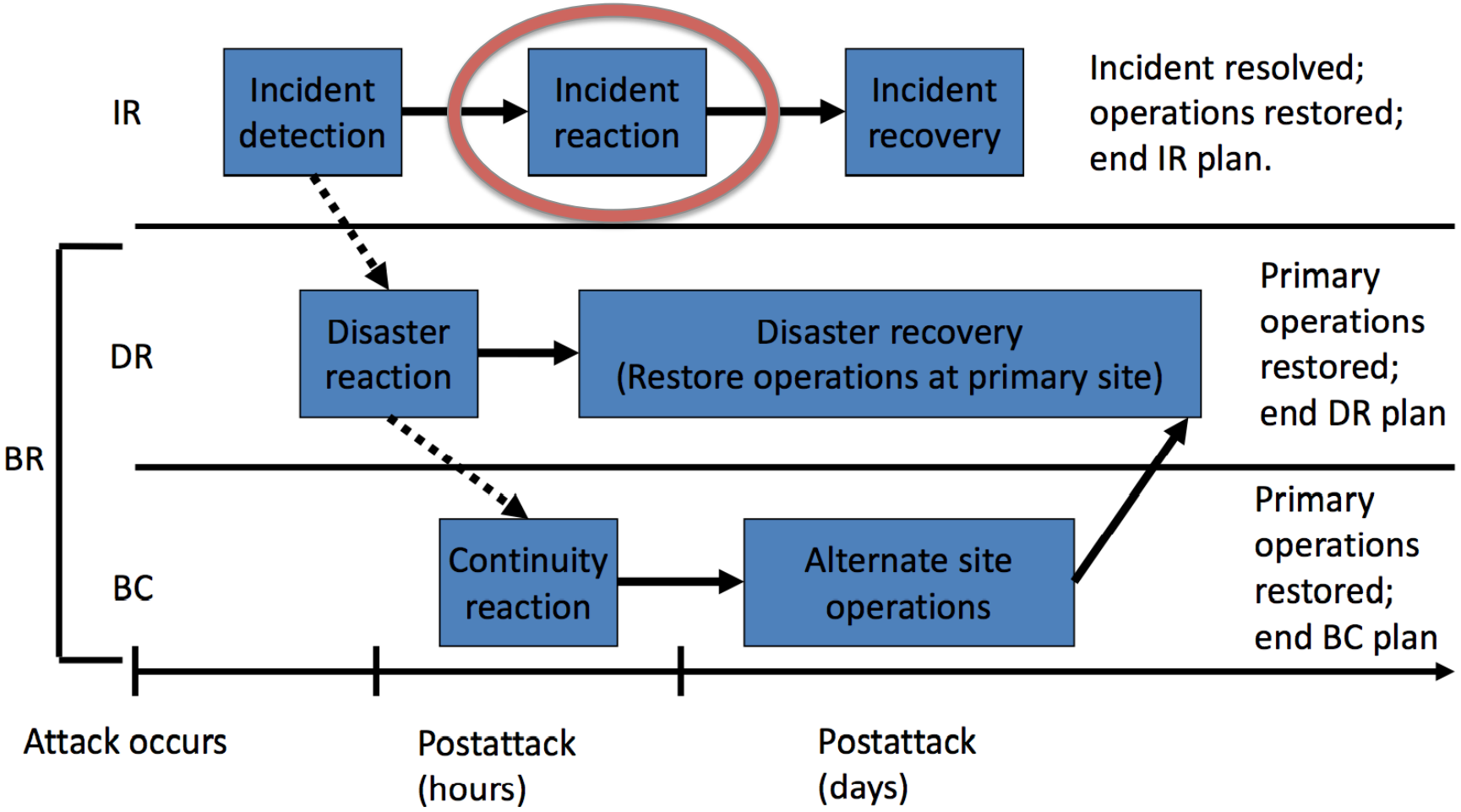
INDICATORS THAT MAY TRIGGER THE IR PLAN

- A phone call or email from a **user**
- Notification from a **network administrator**
- Notification from an **intrusion detection device**
- Review of system **log files** reveal a suspicious pattern
- **Loss** of system connectivity
- Device **malfunctions**

Other specific identifiable situations that result in the IR team leader or IR duty officer to determine that the IR plan must be activated (incident **escalation** following a **triage**)


Email
Other
Triage
IDS
Hotline/Helpdesk
Call Center
Information
Request
Incident
Report
Vulnerability
Report
Analyze
Obtain Contact
Information
Resolution
Coordinate
information
& Response
Provide Technical
Assistance

TIMELINE FOR CONTINGENCY PLAN EXECUTION



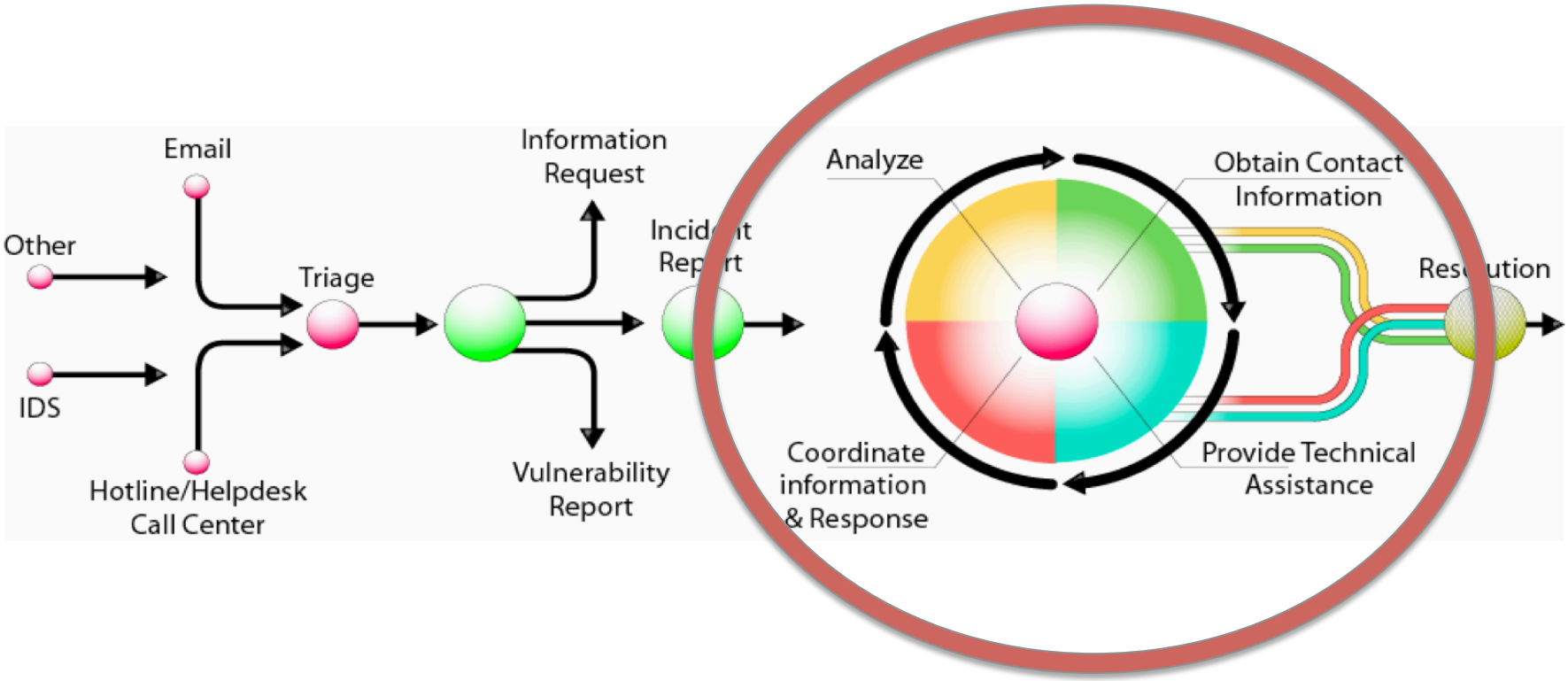
THE CSIRT REACTION FORCE

The IR plan should specify the **team leader** for each particular type of incident, as well as

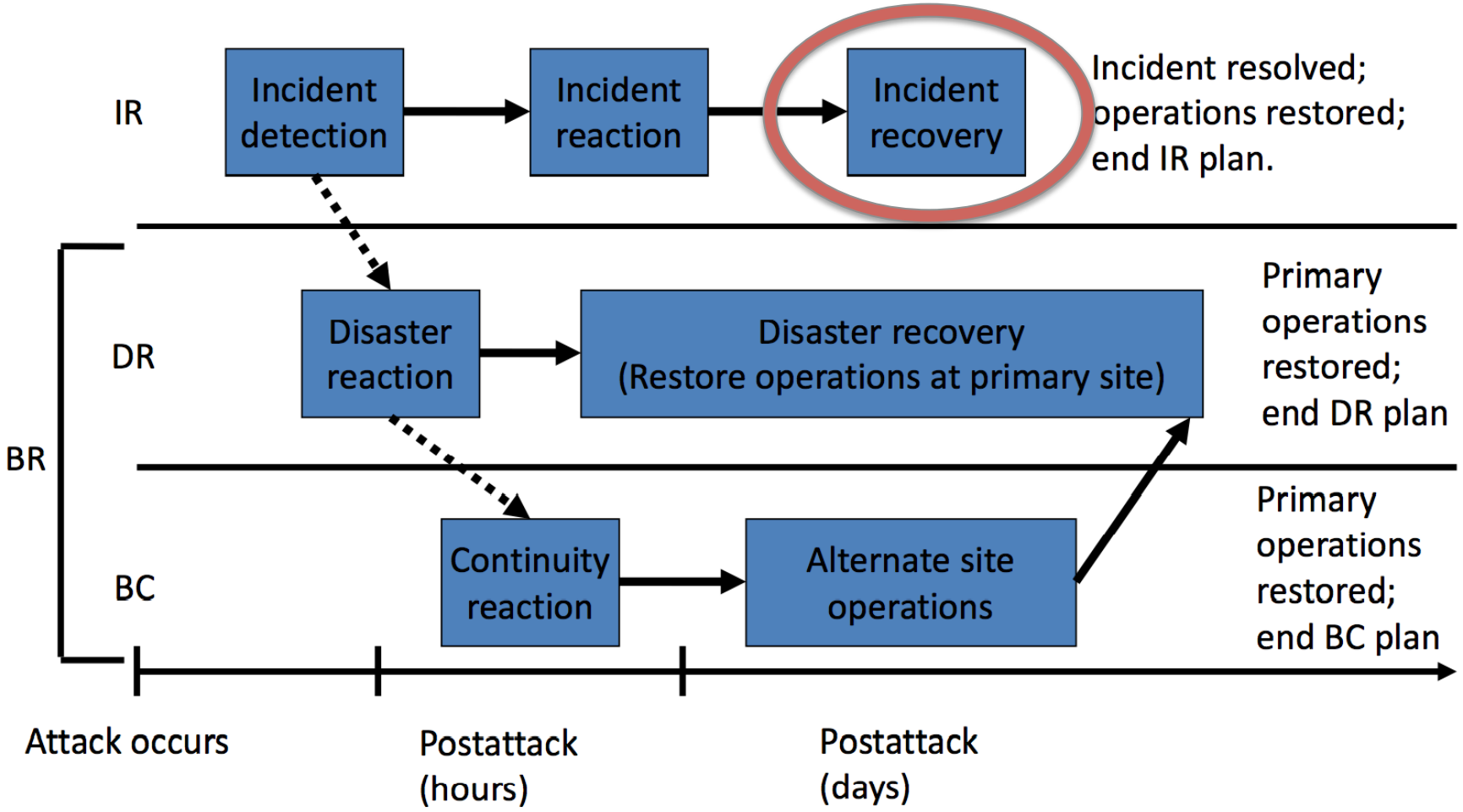
- the **historian** for the event (who maintains logs), and
- **incident handlers**
  - Who and how many determined by the attack scenario for a specific incident

ACTIONS TAKEN DURING THE INCIDENT

- The IR plan must specify how a specific attack scenario should be reacted to
- How depends on **scenario**
- Generally includes:
  - Finding out what happened (incident analysis)
    - *Log analysis, IDS event analysis, …*
    - *Possibly malware analysis, forensic analysis*
  - Mitigating / containing damage
  - Coordination of information and response


Email
Other
IDS
Hotline/Helpdesk
Call Center
Triage
Information
Request
Vulnerability
Report
Analyze
Obtain Contact
Information
Coordinate
information
& Response
Provide Technical
Assistance

TIMELINE FOR CONTINGENCY PLAN EXECUTION



PLANNING FOR AFTER THE INCIDENT

The IR plan must describe:

- Stages necessary to **recover from the events** that will most likely occur as a result of suffering a specific attack scenario
- how to protect from **follow up incidents** (system hardening)
- if **forensic analysis** is to be performed (and possibly how)
- the **after-action** review

PLANNING FOR BEFORE THE INCIDENT

Training the CSIRT:

- Formal training
- Internal training

IR plan testing:

- Desk check
- Structured walk through
- Simulation
- Parallel testing
- Full interruption
- War gaming

frjohnsen Follow

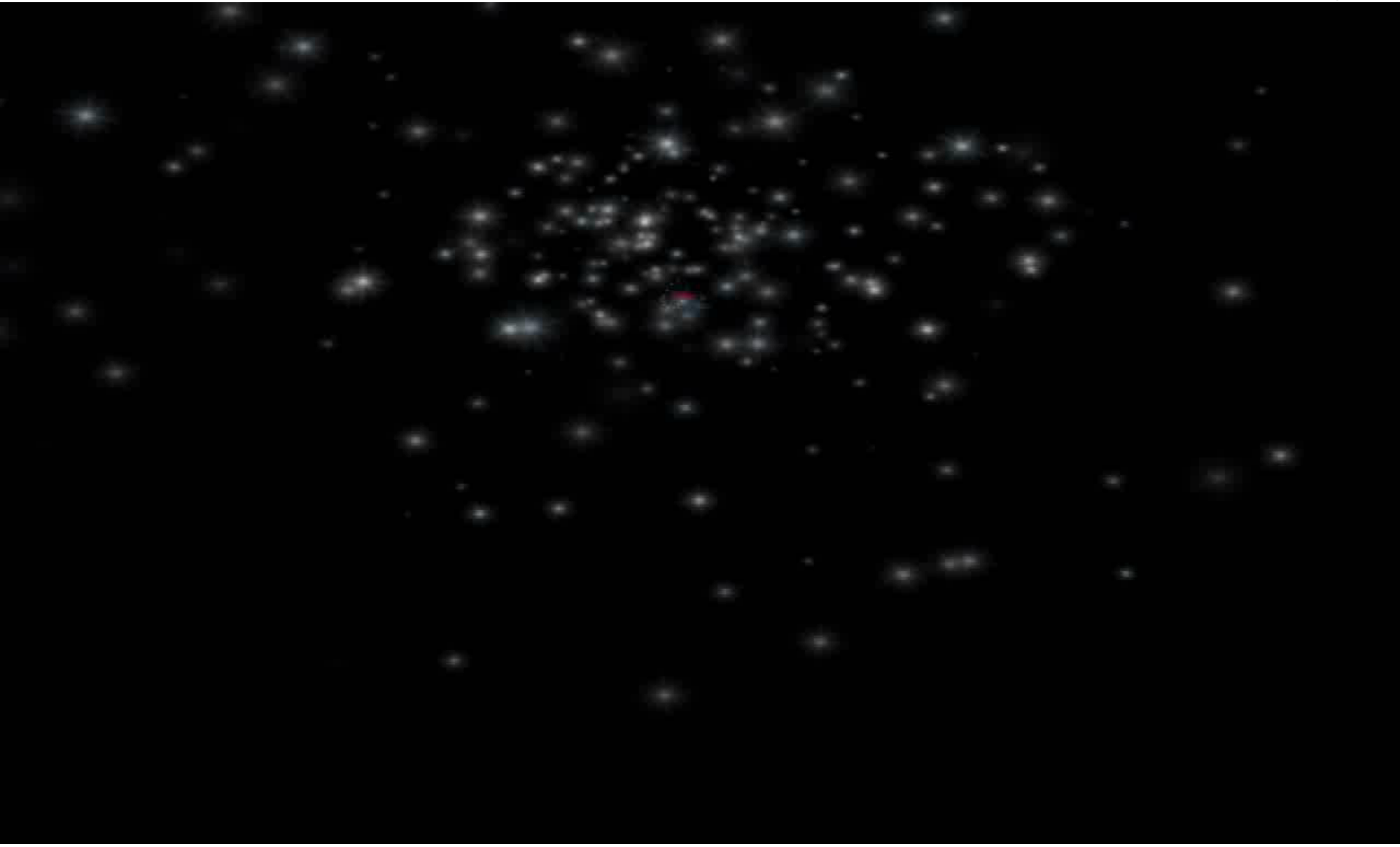
6 months ago

Høy temperatur hos #nsm sitt operasjonssenter under #cyberdawn

rinorock, **karlsruudern**, **emodal** and **10** others like this.

Leave a comment...

http://instagram.com/p/d1oL18Besn/



PREPARING INCIDENT HANDLER COMMUNICATIONS AND FACILITIES

- Contact information
- On-call information
- Incident reporting mechanisms
- Issue tracking system
- Smartphones
- Encryption software
- War room
- Secure storage facility

PREPARING INCIDENT ANALYSIS HARDWARE AND SOFTWARE

- Digital forensics workstations and/or backup devices
- Laptops
- Blank removable media
- Spare workstations, servers, and networking equipment, or the virtualized equivalents
- Portable printer
- Packet sniffers and protocol analyzers
- Digital forensic software
- Removable media with trusted versions of programs for gathering evidence
- Evidence gathering accessories

PREPARING INCIDENT ANALYSIS RESOURCES

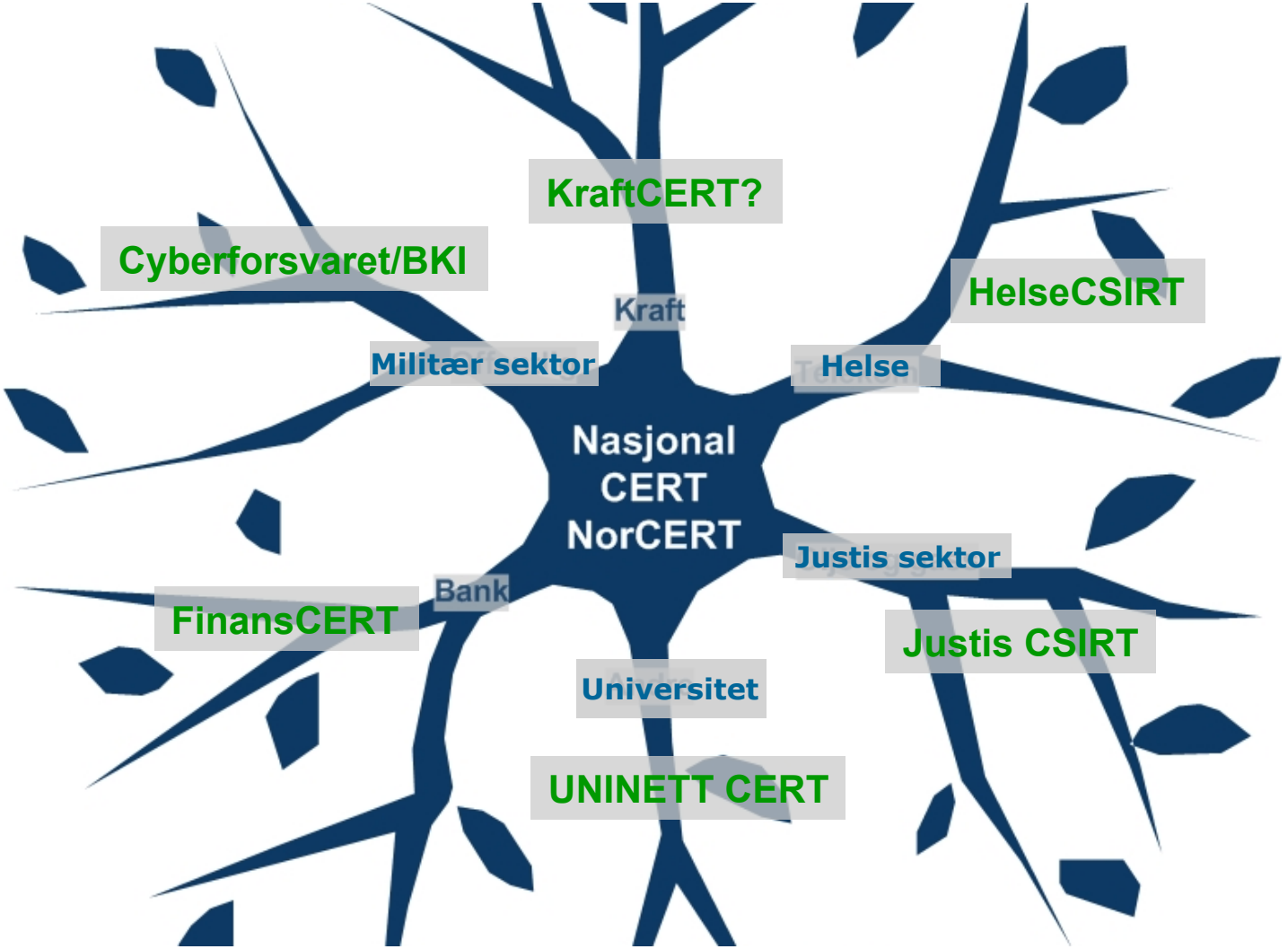
- Port lists
- Documentation
- Network diagrams and lists of critical assets
- Current baselines of expected network, system, and application activity
- Cryptographic hashes of critical files

- Access to images of clean OS and application installations for restoration and recovery purposes

PREPARING FOR COORDINATION AND COMMUNICATION

NIST SP 800-61, Revision 2

SECTORIAL INCIDENT RESPONSE TEAMS IN NORWAY



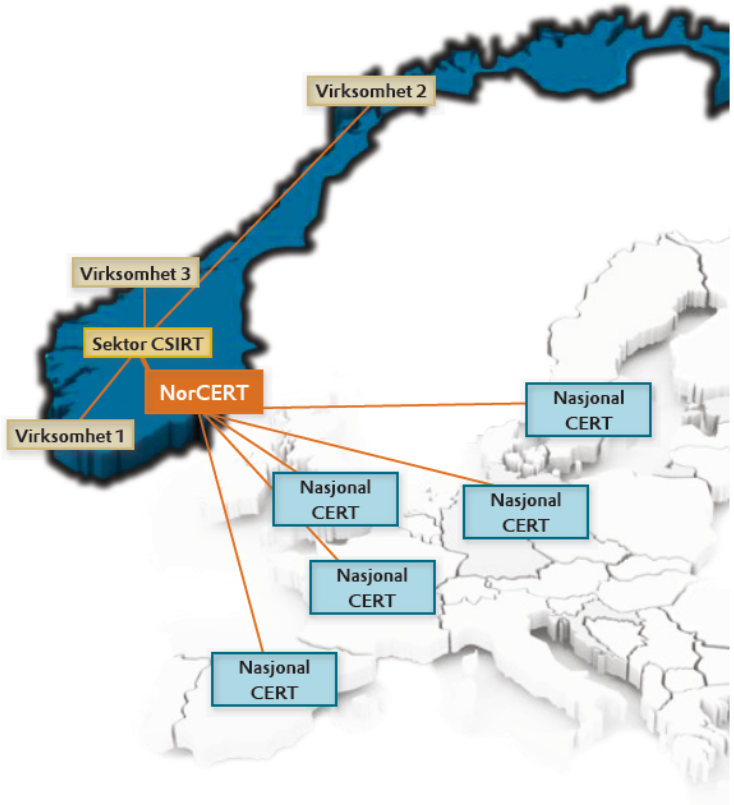
INFORMATION SHARING

Information sharing is crucial to coordinate incident handling across constituencies

- Notification and reports of incidents
- Alerts and advisory distribution
- Sharing of indicators of compromise

There are a number of established information sharing groups

- Open and closed mailing lists/forums
- Membership organizations
- Multi- or bi-lateral collaboration



BUILDING THE SECURITY INCIDENT RESPONSE TEAM

Involves:

- **Collecting information** from stakeholders
  - Identify the incident response need of the organisation
- Defining the IR team **structure**
- Determining the IR team **services**

THE NAME OF THE TEAM

CERT ™ = Computer Emergency Response Team
IRT = Incident Response Team
CSIRT = Computer Security Incident Response Team
CIRT = Computer Incident Response Team
CIRC = Computer Incident Response Capability or Center
SIRT = Security Incident Response Team
SERT = Security Emergency Response Team

ISAC = Information Sharing and Analysis Center
MSSP = Managed Security Service Provider
MSP = Managed Service Providers
ERS = Emergency Response Services
SOC = Security Operations Center
NOC = Network Operations Center

RECOMMENDED STEPS (CERT/CC)

1. Obtain management support and buy-in
2. Determine the CSIRT strategic plan
3. Gather relevant information
4. Design the CSIRT vision
5. Communicate the CSIRT vision and operational plan
6. Begin CSIRT implementation
7. Announce the operational CSIRT
8. Evaluate CSIRT effectiveness

STEP 1: MANAGEMENT SUPPORT AND BUY-IN

- Any organization-wide effort will fail without management support
- Avoid conflict with primary job-responsibilities for those that are assigned part-time roles
- Establish formal support and funding to buy tools
- Constant and on-going support is needed
- The CIO is a natural function-owner for the planning and operation of the CSIRT

STEP 2: DETERMINING THE CSIRT STRATEGIC PLAN

- *Time frame* for the development of the CSIRT
- Gap analysis of needed versus available *personnel resources* (skills)
- CSIRT *structure and team model*
- Available and needed *funding* for initial and ongoing CSIRT operations
- *Training and testing* methods and requirements for the CSIRT
- Formal and informal *communication requirements* between the CSIRT and existing IT/infoSec operations, organizational management, and other responsible individuals
- *Procedures for updating* and modifying CSIRT documents and activities, including findings from training and testing methods

WHAT SKILLS ARE NEEDED IN A CSIRT?

- Malware scanning, elimination and recovery
- System administration
- Network administration
- Firewall administration
- Intrusion detection systems
- Cryptography
- Data storage and recovery
- Malware analysis
- Forensic analysis
- Scripting and coding
- Documentation creation and maintenance
- Creating and following policy and plans
- Teamwork skills
- Communication skills
- Writing skills
- Speaking skills

CSIRT STAFF INTERPERSONAL SKILLS

- Common sense to make efficient and acceptable decisions whenever there is no clear ruling available and under stress or severe time constraints
- Effective oral and written communication skills (in native language and English) to interact with constituents and other teams
- Diplomacy when dealing with other parties, especially the media and constituents
- Ability to follow policies and procedures
- Willingness to continue education
- Ability to cope with stress and work under pressure
- Team player
- Integrity and trustworthiness to keep a team's reputation and standing
- Willingness to admit to one's own mistakes or knowledge limitations about a topic
- Problem solving to address new situations and efficiently handle incidents
- Time management, in order to concentrate on priority work

EXAMPLES OF CSIRT STAFF ROLES

Incident Handler Officer

Analyst

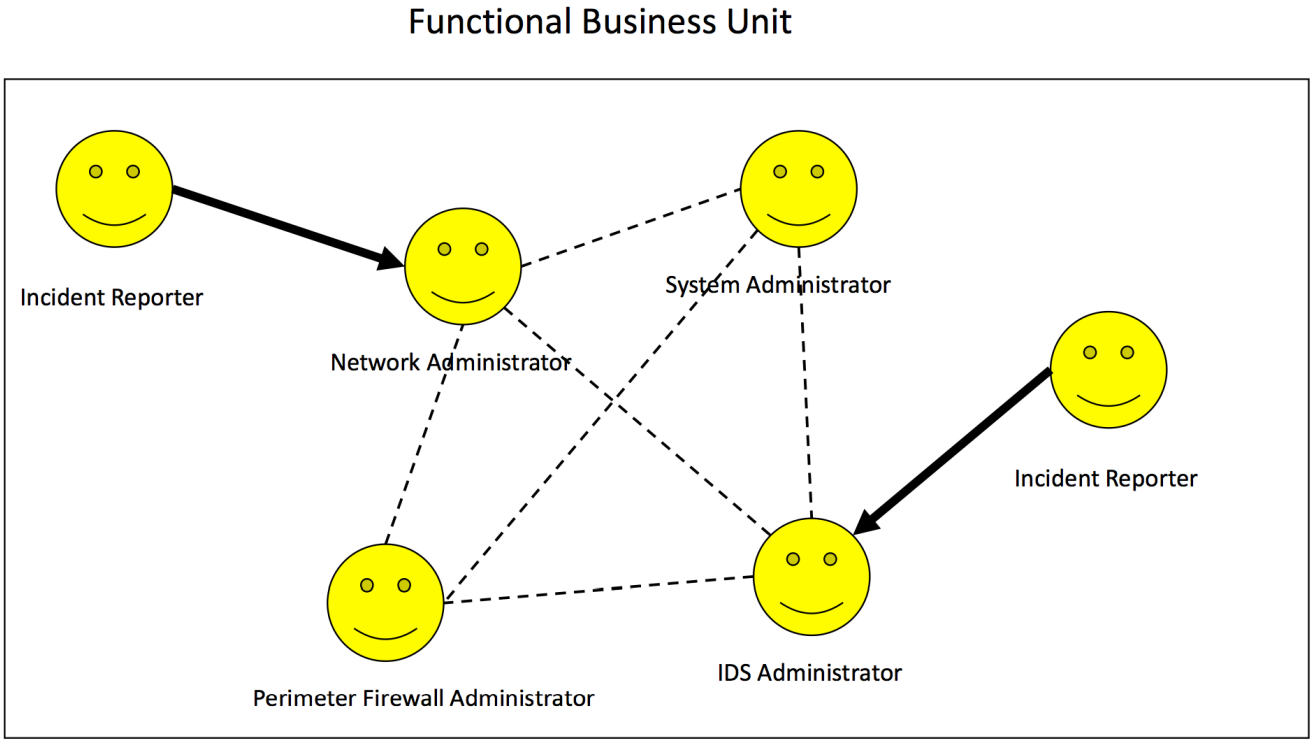
Watch Officer

CSIRT STRUCTURE AND TEAM MODEL

- Security Team
- Distributed CSIRT
- Centralized CSIRT
- Combined Distributed and Centralized CSIRT
- Coordinating CSIRT

CSIRTS may be staffed by employees, partially outsourced or fully outsourced.

SECURITY TEAM MODEL

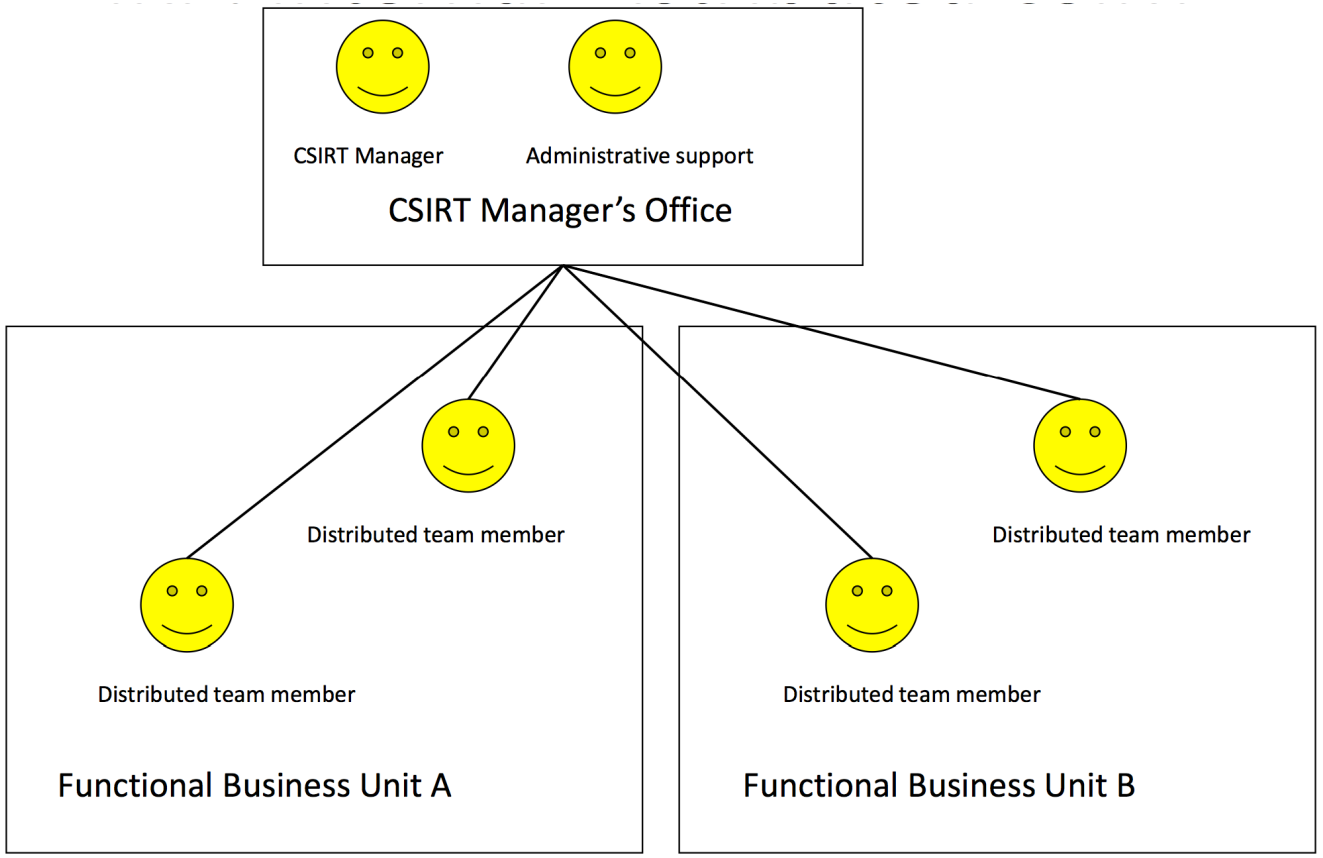


Adapted from Organizational Models for CSIRTs

SECURITY TEAM MODEL

Staff	•Requires no additional staffing, utilises existing personnel such as network administrators.
Equipment	•No additional equipment needed. •Existing equioment is used.
Infrastructure	No new infrastructure needed, existing infrastructure is used.
Strenghts of the model	•No real strenghts in this model. •No additional costs incurred (but likely offset by damage from incidents).
Weaknesses of the model	•Non-standard or multiple routines for reporting makes users unsure of where and if they should report incidents. •Lack of coordination means categorisation and analysis of information is handled inconsistently across the organisation. •Poor overview of available expertise. •Difficult to determine problem ownership. •May result in incorrect incident evaluation.

DISTRIBUTED CSIRT

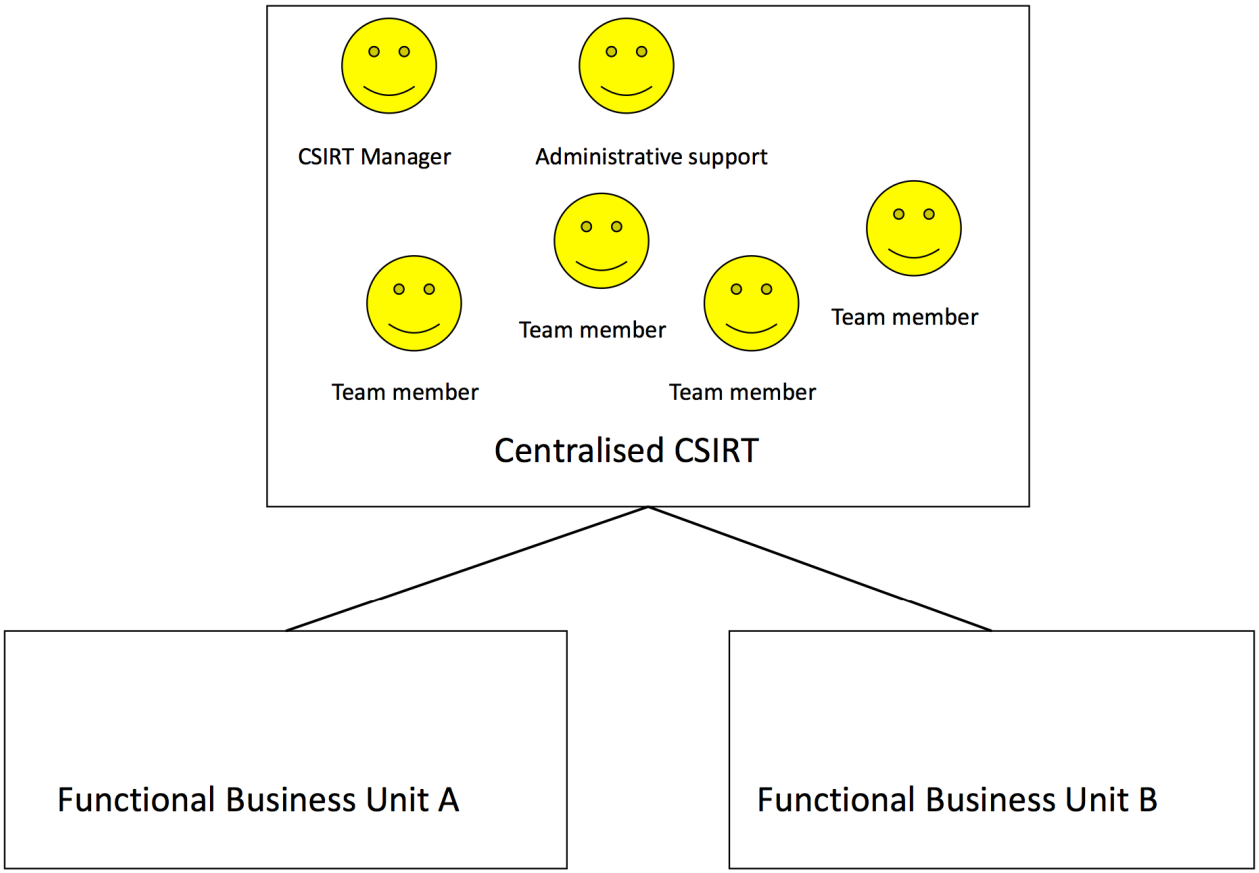


Adapted from Organizational Models for CSIRTs

DISTRIBUTED CSIRT

Strenghts of the model	•The incident management process is coordinated, which means security policies can be set and enforced enterprise-wide. •Centralised tracking system and repository of data. •The distributed nature of the team means individual team members are well attuned to local operations and conditions.
Weaknesses of the model	•Staff may have split responsibilities and not work full time in the CSIRT. •Time and energy is needed to gain and keep skills current. •If this does not happen, appropriate commitment from operating units may not be sustainable over time. •Effective management and coordination of the distributed team may become a challenge without a strong leader and appropriate upper management support. •Determining where CSIRT authority lies and the willingness of other divisions to accept that authority may be difficult. •Communication across a distributed CSIRT may be difficult to achieve in a timely manner.

CENTRALIZED CSIRT



Adapted from Organizational Models for CSIRTs

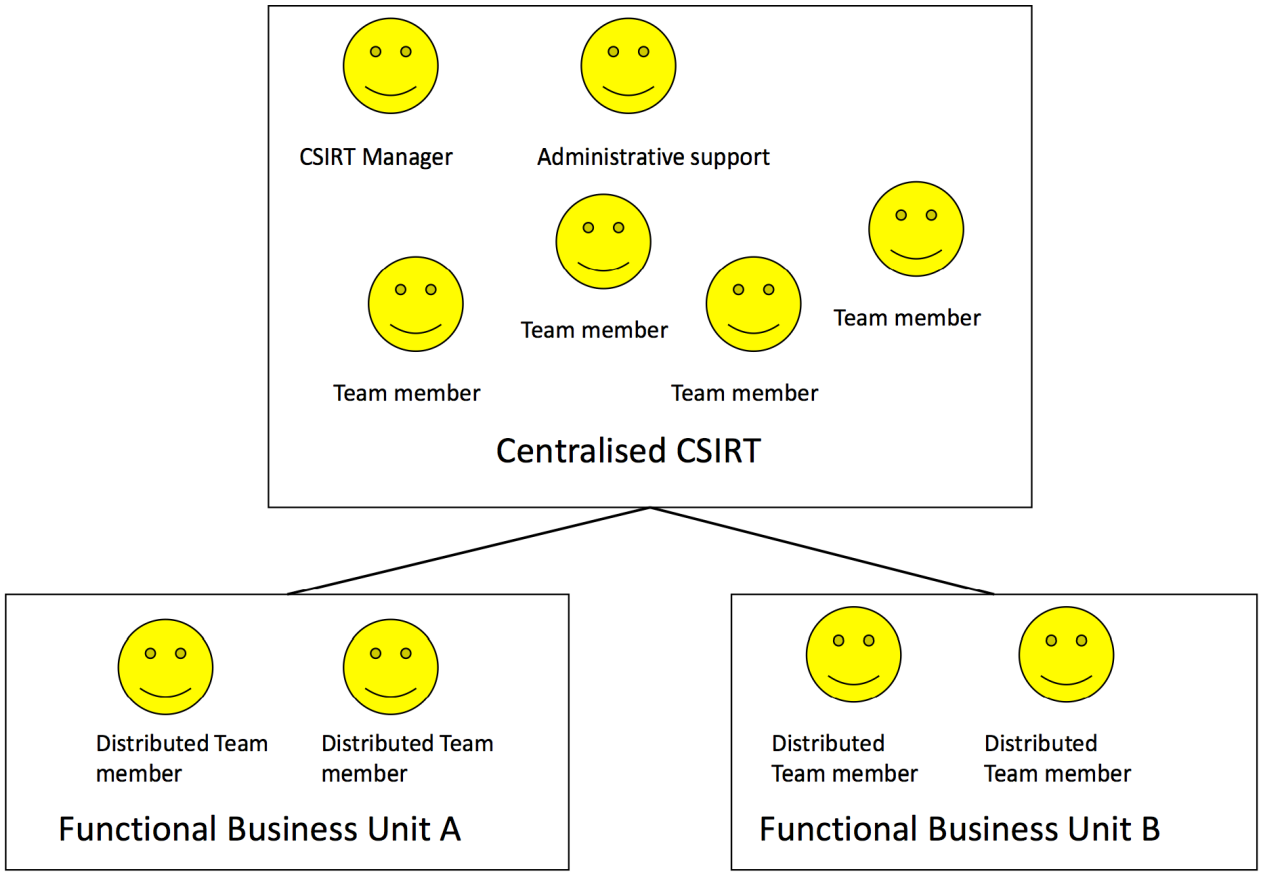
CENTRALIZED CSIRT

Strenghts of the model	•Team members do not have to divide time between CSIRT activities and other duties. •Dedicated staff with dedicated training in incident management. •Central repository for all incident related information, facilitates enterprise-wide analysis. •Possible to build a comprehensive knowledgebase of incident and vulnerability reports, analysis and response strategies.

CENTRALIZED CSIRT

Weaknesses of the model	•It may be difficult to coordinate with distant sites. •Strong management support is required so that the team does not become isolated from the rest of the organisation. •Additional budget is needed. •It may be difficult to find the correct team size •In large organisations it may be difficult for the team to obtain expertise in all technologies and systems used. •It is challenging to provide the team with up to date operational information on the organisation's critical infrastructure. •It is difficult to ensure that all divisions act on information in a timely manner. •Information may have to flow through several hierarcical levels to reach appropriate individuals, causing delays in response and recovery. •Incident handling knowledge is consolidated in a few individuals. Massive loss of knowledge when they leave.

COMBINED DISTRIBUTED AND CENTRALIZED CSIRT



Adapted from Organizational Models for CSIRTs

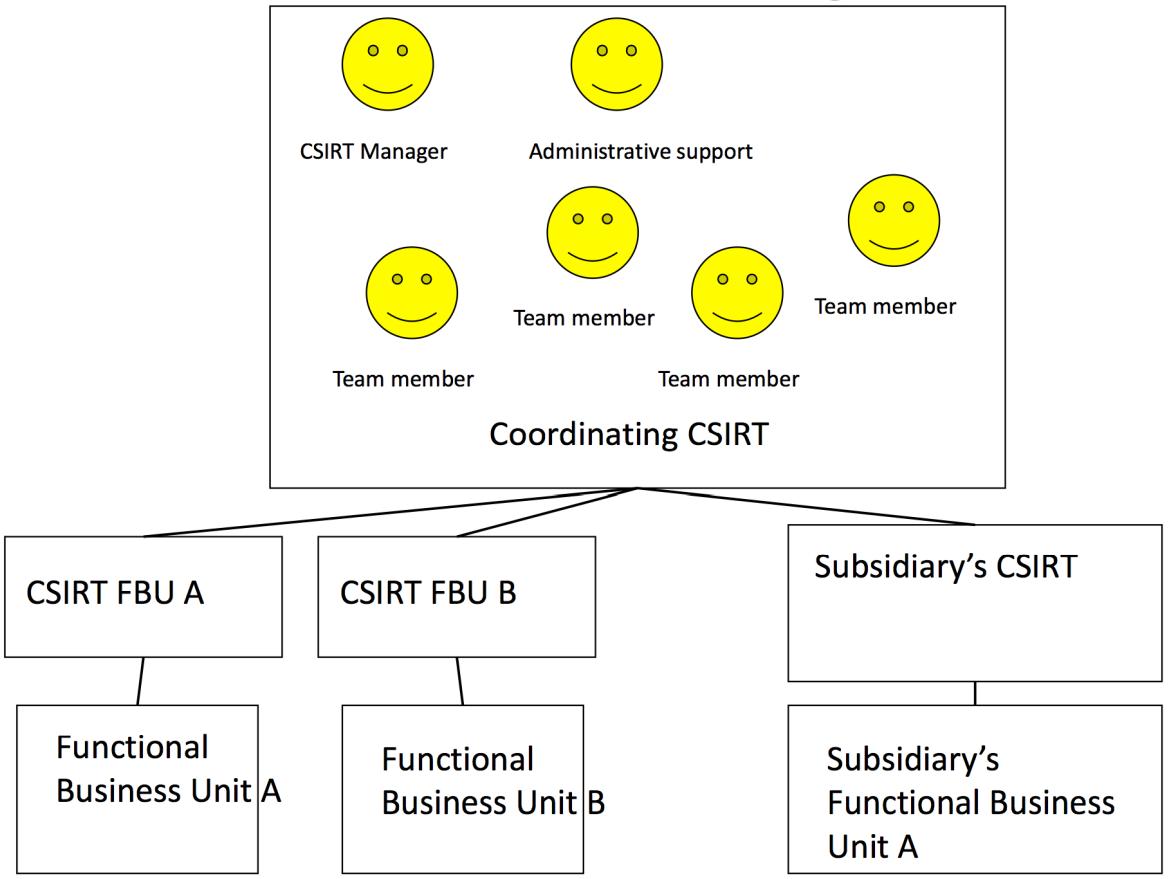
COMBINED DISTRIBUTED AND CENTRALIZED CSIRT

Strenghts of the model	•CSIRT functions are performed by a focused dedicated staff, who are trained in security incident response and recovery. •The distributed team members support the centralised team, providing expertise in local and systems operations. •There is coordinated incident reporting, analysis, and response across the enterprise. •There is a centralized responsibility for synthesising and analysing information to detect trends across the enterprise. •There is a central repository for incident, vulnerability, and artifact data and related information. •The CSIRT is able to use this information to provide valuable guidance and recommendations to the constituency. •This model facilitates the implementation of organisation-wide computer security guidelines and procedures.

COMBINED DISTRIBUTED AND CENTRALIZED CSIRT

Weaknesses of the model	•It is difficult to coordinate with all geographic and divisional sites. •The centralised team may seem isolated from the rest of the organisation. •The distributed team may believe responsibility rests with the centralised members. •The organisation may have to fill new positions and purchase new equipment. •It is difficult to determine the correct size of CSIRT staff. •Depending on the location of the centralised CSIRT, it may difficult to get other divisions to follow recommendations. •It is difficult to manage and coordinate coverage in all necessary areas of expertise. •Information may have to flow through several hieararchical levels, which may cause delays in implementation of recommendations and incident handling and recovery.

COORDINATING CSIRT



Adapted from Organizational Models for CSIRTs

COORDINATING CSIRT

Strenghts of the model	•There is a dedicated staff trained in computer security response and coordination. •There is a focused, dedicated responsibility for performing incident response coordination. •There is a central point for incident reporting, analysis, and response across the organizations in the constituency. •There is a central point for analyzing information to determine trends and patterns for the entire constituency. •There is a central repository for incident, vulnerability, and artifact data from the entire constituency. •There is a focal point for incident reporting from outside the constituency where the coordinating CSIRT accepts incoming reports and forwards them, with supporting information, to the organizations involved. •The CSIRT can use the obtained information and analysis to provide valuable information to the constituency (advisories, alerts, warnings, technical documents, checklists, best practices, etc.).

COORDINATING CSIRT

Weaknesses of the model	•It is difficult to coordinate with all entities in large and disperse constituencies. •The coordinating team may seem isolated from the rest of the organizations in the constituency. •The constituency may need to fund the coordinating CSIRT. •It is difficult to determine the correct size of the staff. •It can be difficult to get buy-in from organizations to follow CSIRT recommendations. •It is difficult to manage and coordinate coverage in all the areas of expertise necessary at an in-depth level. •Finding experts in the constituency may be cumbersome, and over time there can be problems with turnover, as well as training issues. •It is difficult to ensure that all entities within the constituency respond to incident reports and act on recommendations in a timely, appropriate manner.

SELECTING CSIRT STRUCTURE AND TEAM MODEL

- Size and Distribution of Constituency
- Services Provided and Related Service Levels
- Funding and Resources
- Position in the Organization

SELECTING THE CSIRT STRUCTURE AND TEAM MODEL

- Is 24/7 availability needed?
- Full time vs. part time members
- Employee morale
- Cost
- Staff expertise
- Organisational structures
- Outsourcing incident response

OUTSOURCING THE CSIRT

Advantages:

- Services provided by professional IR staff
- 24/7 monitoring
- Early notification of potential problems in region
- Formal reports and briefings on attacks and response
- Equipment specified and installed by well trained professionals
- No additional personnel costs or training

OUTSOURCING THE CSIRT

Disadvantages:

- Potential loss of control of response to incidents
- Possible exposure of classified organisational data to service providers
- Locked in to proprietary equipment and services
- Loss of services when contract expires, unless renewed
- Loss of customization to the needs of each organisation
- Organisation's need subjugated to service provider's needs
- More important / prestigious companies given preference in response

STEP 4: DESIGNING THE CSIRT VISION

- Identify your **constituency**
  - *Who does the CSIRT support and serve?*
- Define your CSIRT's **mission, goals and objectives**
  - *What does it do for the identified constituency?*
- Determine the **organizational model**
- Select the **CSIRT services** to provide to the constituency
- Identify **required resources**
- Determine your CSIRT **funding**

CSIRT SERVICES

Reactive services:

- Incident response
- *Triggered by an event or request*, such as a report of a compromised host, wide-spreading malicious code, software vulnerability, or something that was identified by an intrusion detection or logging system.
- Core component of CSIRT work

Based on CSIRT Services. (c) Carnegie Mellon University.

CSIRT SERVICES

Proactive services:

- Provide assistance and information to help *prepare, protect, and secure constituent systems* in anticipation of attacks, problems, or events.
- Will *directly reduce* the number of incidents in the future.

Based on CSIRT Services. (c) Carnegie Mellon University.

CSIRT SERVICES

Security quality management services:

- Augment existing and well-established services that are independent of incident handling and traditionally performed by other areas of an organization such as the IT, audit, or training departments.
- The CSIRT's point of view and expertise can provide insight to help improve the overall security of the organization and identify risks, threats, and system weaknesses.
- Generally proactive but contribute indirectly to reducing the number of incidents.

Based on CSIRT Services. (c) Carnegie Mellon University.

Reactive Services

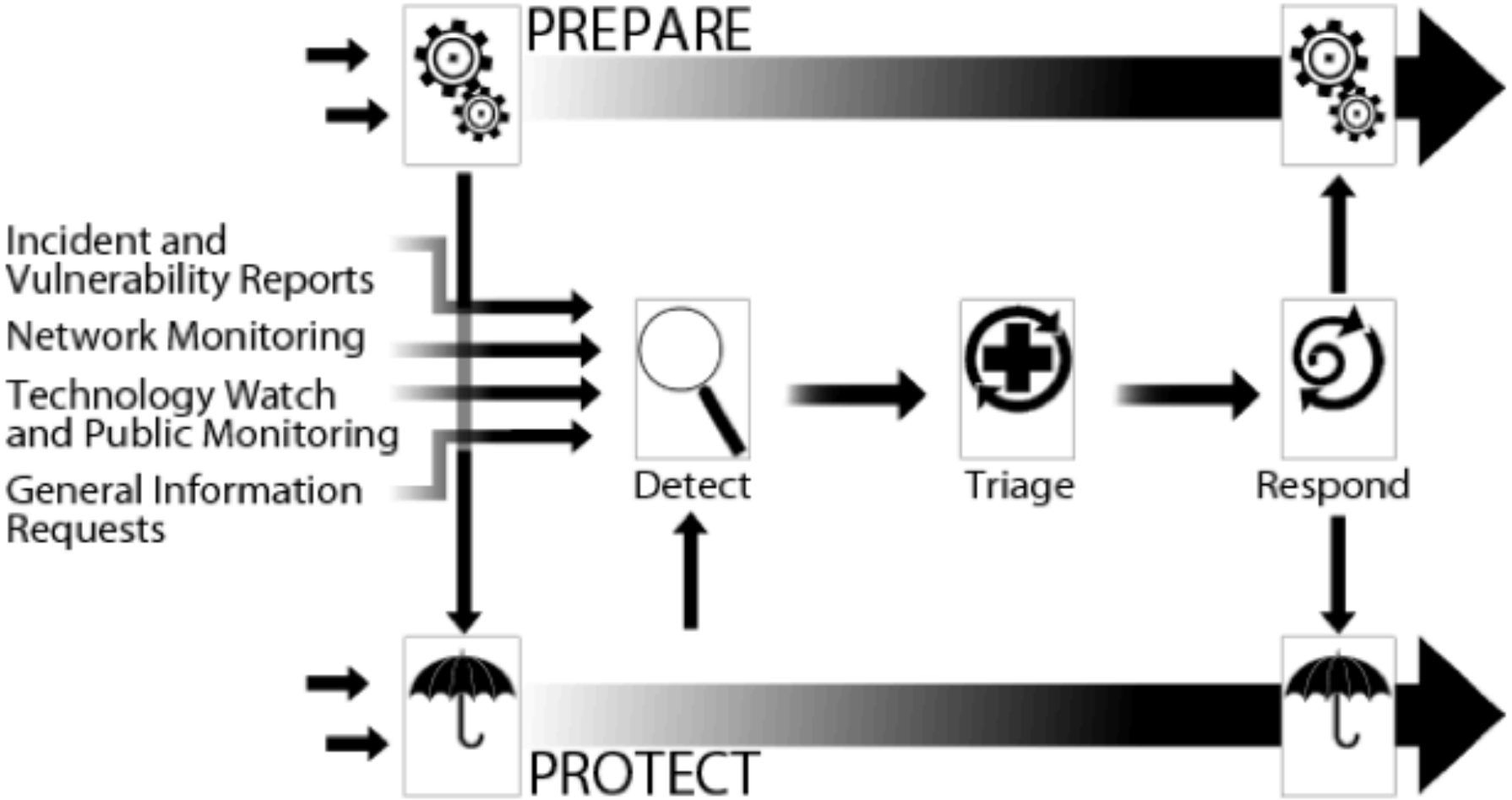
- Alerts and Warnings
- Incident Handling
  - –Incident analysis
  - –Incident response on site
  - –Incident response support
  - –Incident response coordination
- Vulnerability Handling
  - –Vulnerability analysis
  - –Vulnerability response
  - –Vulnerability response coordination
- Artifact Handling
  - –Artifact analysis
  - –Artifact response
  - –Artifact response coordination

Proactive Services

- Announcements
- Technology Watch
- Security Audit or Assessments
- Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

Security Quality Management Services

- ✓Risk Analysis
- ✓Business Continuity & Disaster Recovery Planning
- ✓Security Consulting
- ✓Awareness Building
- ✓Education/Training
- ✓Product Evaluation or Certification



Source: CERT/CC Defining Incident Management Processes for CSIRTs: A Work in Progress

REACTIVE SERVICES: ALERTS AND WARNINGS

- **Disseminating information** that describes an intruder attack, security vulnerability, intrusion alert, computer virus, or hoax

- Providing any short-term recommended course of action for dealing with the resulting problem

Based on CSIRT Services. (c) Carnegie Mellon University.

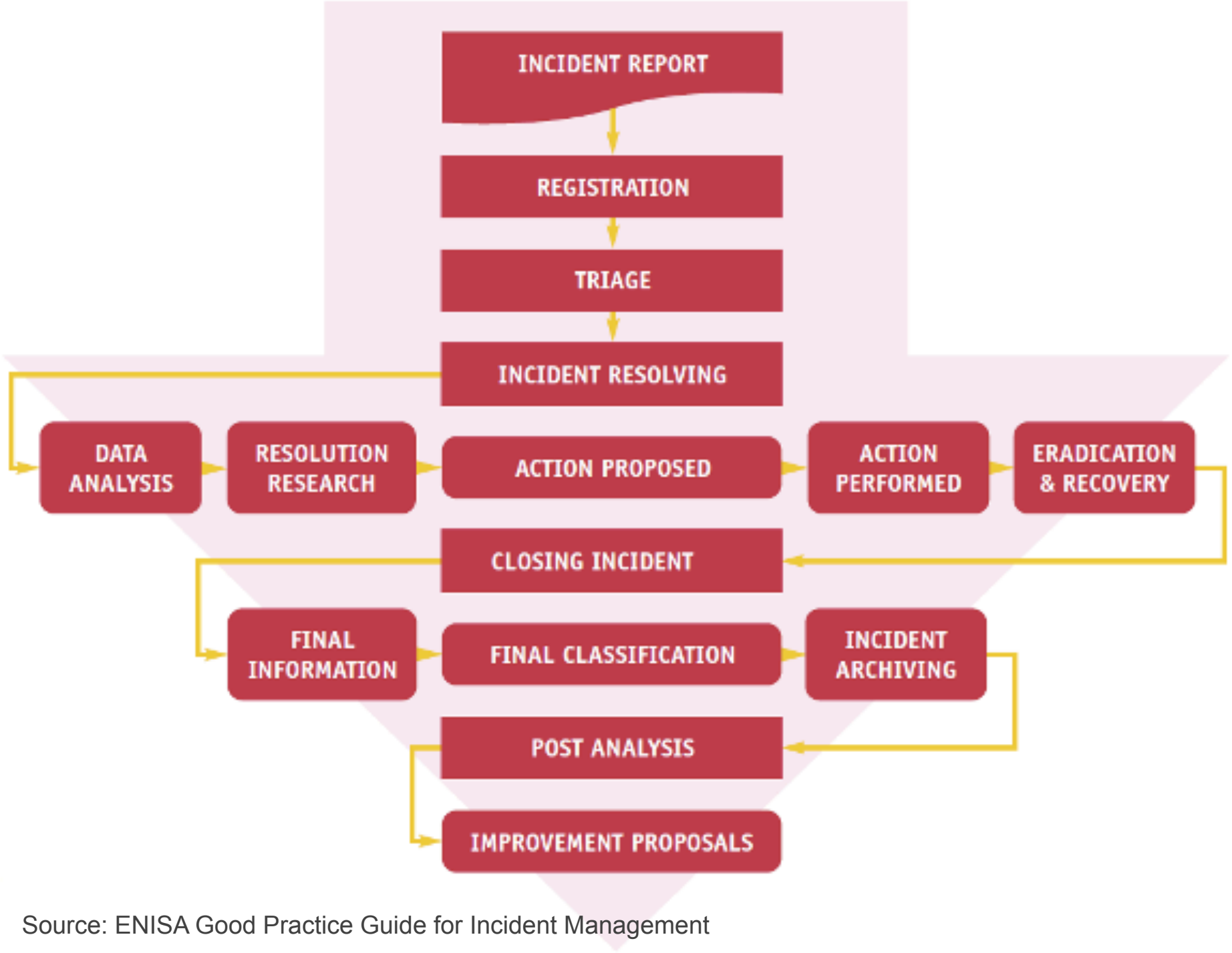
REACTIVE SERVICES: INCIDENT HANDLING

Receiving, triaging, and responding to requests and reports, and analyzing incidents and events.

Can include:

- **Taking action to protect** systems and networks affected or threatened by intruder activity
- Providing solutions and **mitigation strategies** from relevant advisories or alerts
- **Looking** for intruder activity on other parts of the network
- **Filtering** network traffic
- **Rebuilding** systems
- **Patching** or repairing systems
- **Developing** other response or workaround strategies

Based on CSIRT Services. (c) Carnegie Mellon University.



Source: ENISA Good Practice Guide for Incident Management

REACTIVE SERVICES: INCIDENT ANALYSIS

An examination of all available information and supporting evidence or artifacts related to an incident or event.

The purpose is to identify the scope of the incident, the extent of damage caused by the incident, the nature of the incident, and available response strategies or workarounds.

Forensic evidence collection:

- Collection, preservation, documentation, and analysis of evidence from a compromised computer system to determine changes to the system and to assist in the reconstruction of events leading to the compromise

Tracking or tracing:

- Tracing the origins of an intruder or identifying systems to which the intruder had access
- This work might be done alone but usually involves working with law enforcement personnel, Internet service providers, or other involved organizations

Based on CSIRT Services. (c) Carnegie Mellon University.

REACTIVE SERVICES: INCIDENT RESPONSE

Incident response on site:

- Direct, on-site assistance to help constituents recover from an incident

Incident response support:

- Assists and guide the victim(s) of the attack in recovering from an incident via phone, email, fax, or documentation
- Can involve technical assistance in the interpretation of data collected, providing contact information, or relaying guidance on mitigation and recovery strategies

Based on CSIRT Services. (c) Carnegie Mellon University.

REACTIVE SERVICES: INCIDENT RESPONSE COORDINATION

Coordinate the response effort among parties involved in the incident.

Usually includes:

- The victim of the attack
- Other sites involved in the attack
- Any sites requiring assistance in the analysis of the attack
- It may also include the parties that provide IT support to the victim, such as Internet service providers, other CSIRTs, and system and network administrators at the site.

May involve notification and collaboration with:

- Legal counsel
- Human resources
- Public relations departments
- Law enforcement.

Based on CSIRT Services. (c) Carnegie Mellon University.

REACTIVE SERVICES: VULNERABILITY HANDLING

- Receiving information and reports about hardware and software vulnerabilities
- Analyzing the nature, mechanics, and effects of the vulnerabilities
- Developing response strategies for detecting and repairing the vulnerabilities

Based on CSIRT Services. (c) Carnegie Mellon University.

REACTIVE SERVICES: ARTIFACT HANDLING

*An **artifact** is any file or object found on a system that might be involved in probing or attacking systems and networks or that is being used to defeat security measures.*

- Can include but is not limited to computer viruses, Trojan horse programs, worms, exploit scripts, and toolkits.

Artifact analysis:

- Technical examination and analysis of any artifact found on a system.

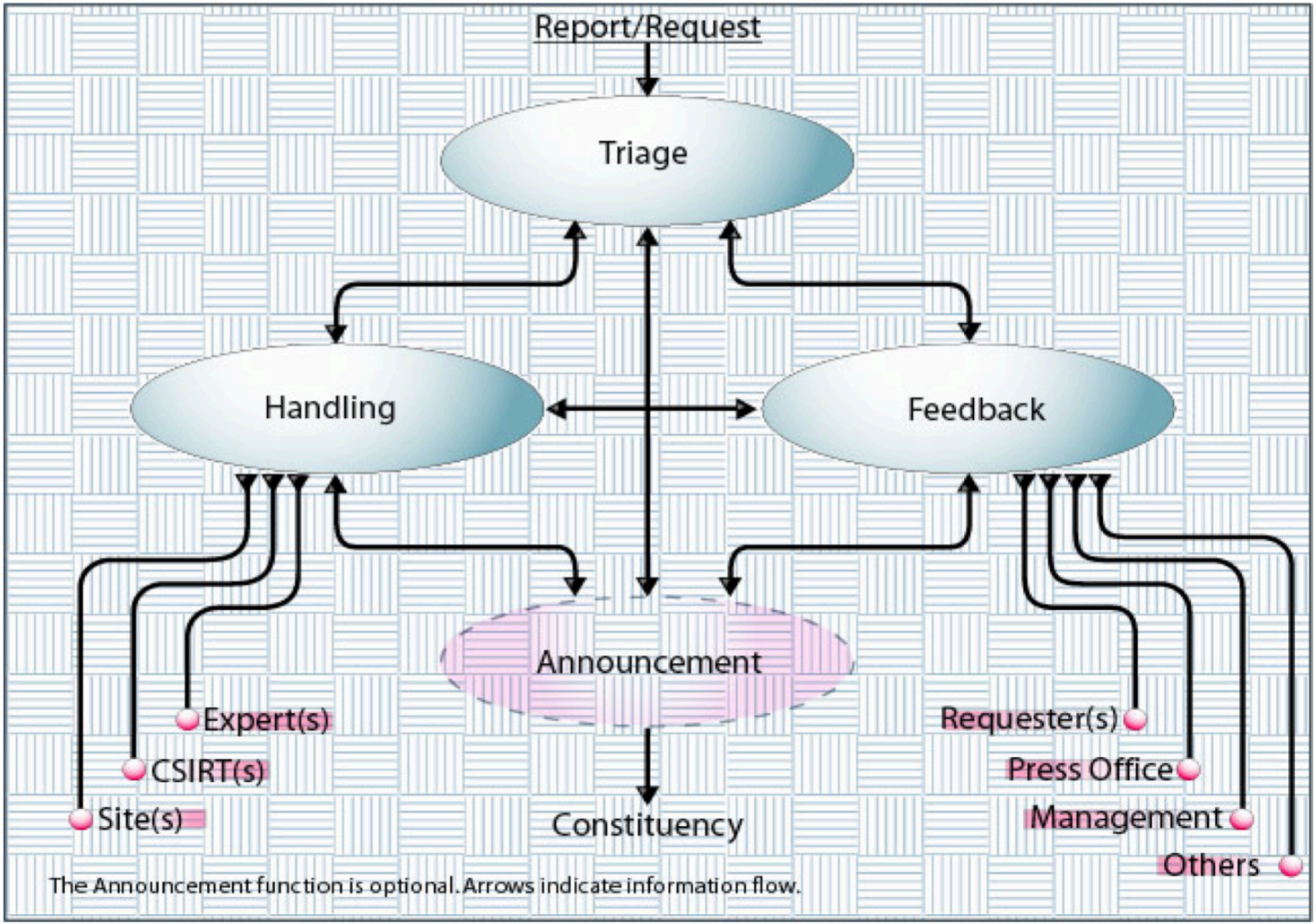
Artifact response:

- Determining appropriate actions to detect and remove artifacts from a system, as well as actions to prevent artifacts from being installed.

Artifact response coordination:

- Sharing and synthesizing analysis results and response strategies pertaining to an artifact with other researchers, CSIRTs, vendors, and other security experts.

Based on CSIRT Services. (c) Carnegie Mellon University.



Handbook for Computer Incident Response Teams (CSIRTS)

CSIRT PROACTIVE SERVICES

Announcements

- Intrusion alerts, vulnerability warnings, and security advisories

Technology Watch

- Monitoring and observation of new technical developments, intruder activities, and related trends to help identify future threats
- Can be expanded to include legal and legislative rulings, social or political threats, and emerging technologies

Based on CSIRT Services. (c) Carnegie Mellon University.

TECHNOLOGY WATCH: REPORTS TO WATCH OUT FOR

2013

APT1

Hangover

NetTraveler

2014

Ke3chang

The Mask

Red October

Miniduke

Sunshop

CSIRT PROACTIVE SERVICES

Security Audits or Assessments

- Review and analysis of an organization's security infrastructure, based on the requirements defined by the organization or by other industry standards

Configuration and Maintenance of Security Tools, Applications, Infrastructures, and Services

- Identify or provide appropriate guidance on how to securely configure and maintain tools, applications, and the general computing infrastructure used by the CSIRT constituency or the CSIRT itself
- Configuration updates and maintenance of security tools and services, such as IDS, network scanning or monitoring systems, filters, wrappers, firewalls, virtual private networks (VPN), or authentication mechanisms
- Configure and maintain servers, desktops, laptops, personal digital assistants (PDAs), and other wireless devices according to security guidelines

Based on CSIRT Services. (c) Carnegie Mellon University.

CSIRT PROACTIVE SERVICES

Security-Related Information Dissemination

- Reporting guidelines and contact information for the CSIRT
- Archives of alerts, warnings, and other announcements
- Documentation about current best practices
- General computer security guidance
- Policies, procedures, and checklists
- Vendor links
- Current statistics and trends in incident reporting
- Other information that can improve overall security practices

Based on CSIRT Services. (c) Carnegie Mellon University.

CSIRT QUALITY MANAGEMENT SERVICES

Security Quality Management Services:
Well-known, established services designed to improve the overall security of an organization.

Risk Analysis
The CSIRTs experience and expertise may:

- Improve the organization's ability to assess real threats
- Provide realistic qualitative and quantitative assessments of the risks to information assets
- Help to evaluate protection and response strategies

Business Continuity and Disaster Recovery Planning

Based on CSIRT Services. (c) Carnegie Mellon University.

CSIRT QUALITY MANAGEMENT SERVICES

Security Consulting:

- Provide advice and guidance on the **best security practices** to implement for constituents' business operations
- Involves preparing recommendations or identifying requirements for purchasing, installing, or securing new systems, network devices, software applications, or enterprise-wide business processes
- Providing guidance and assistance in developing organizational or constituency security policies
- Testimony or advice to legislative or other government bodies.

Based on CSIRT Services. (c) Carnegie Mellon University.

CSIRT QUALITY MANAGEMENT SERVICES

Awareness Building

- CSIRTs may be able to identify where constituents require more information and guidance to better conform to accepted security practices and organizational security policies.

Education/Training

- Providing information to constituents about computer security issues through seminars, workshops, courses, and tutorials.
- Topics might include incident reporting guidelines, appropriate response methods, incident response tools, incident prevention methods, and other information necessary to protect, detect, report, and respond to computer security incidents.

Based on CSIRT Services. (c) Carnegie Mellon University.

CSIRT QUALITY MANAGEMENT SERVICES

Product Evaluation or Certification

- Conduct product evaluations on tools, applications, or other services to ensure the security of the products and their conformance to acceptable CSIRT or organizational security practices.

STEP 6: BEGINNING CSIRT IMPLEMENTATION

- Recruit and train initial **CSIRT staff**
- Purchase **equipment** and prepare the required **network infrastructure**
- Define and prepare the necessary CSIRT **policies and procedures**
- Define and acquire your **incident-tracking system**
- Prepare **incident-reporting guidelines** and forms

STEP 7: ANNOUNCE THE OPERATIONAL CSIRT

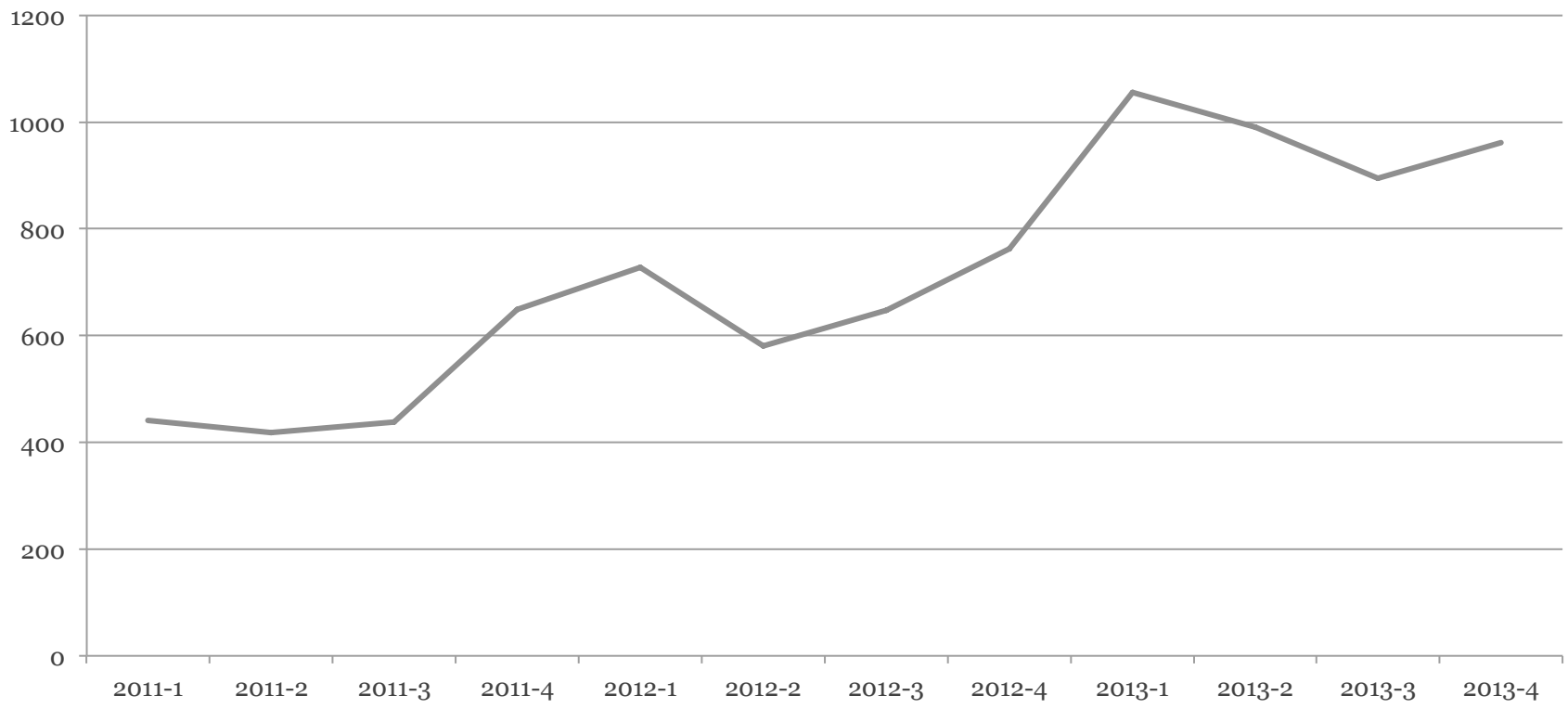
- Staff members and leadership
- Mission and goals
- Services and functions
- Operating hours
- Contact methods and numbers

STEP 8: EVALUATING CSIRT EFFECTIVENESS

CSIRT performance measures:

- *Comparison* of local CSIRT measures to other CSIRTs
- Solicitation of *comments* from the CSIRTs constituency
- Using *periodic surveys* to gain insight from the CSIRT constituency
- Definition of a set of *empirical measures* that can be collected, reported and audited to evaluate the team
  - Incidents reported
  - Response times
  - Resolution rates

EXAMPLE: NUMBER OF INCIDENTS HANDLED AT NORCERT



CLOSING THE LOOP

After-action review:

- A detailed examination of the events that occurred during an incident, from first detection to final recovery
- All key players review their notes and verify that the documentation is accurate
- The goal is to identify areas where the IR plan worked, didn't work or should be improved
- This allows the IR to be updated as needed
- The group should use extreme care to avoid finger-pointing and blame-casting
- Should be performed at the end of every major incident
- Can also serve as a training case for future staff

HOW TO COUNTERACT STAFF BURNOUT?

- Budget enough funding for maintaining skills
  - Sending team-members to technical conferences
- Ensure the availability of books, magazines and other technical references
- Give team members the opportunity to perform other tasks
  - Conducting research, write software, conduct workshops, …
- Consider rotating staff members
- Maintain sufficient staffing
- Create mentoring programs
- Participate in exchanges where team members temporarily trade places to gain new technical skills
- Bring in outside experts with deep technical knowledge
- Conduct simulated incident handling exercises

NEXT LECTURE

The topic of the next lecture on the 17th of Mars will be:

Incident Response: Detection and Notification

Recommended reading to prepare for the next lecture:

- Chapter 5 in Whitman, Mattord and Green
- *Proactive detection of network security incidents (ENISA deliverable)*

I also encourage you to set up a VM and install Security Onion for hands-on exercises/demos!
(See Whitman, Mattord and Green 2014 p. 82 for instructions)

Please note that the lecture on the 17th of Mars is from **13:15-15:00** (See TimeEdit)