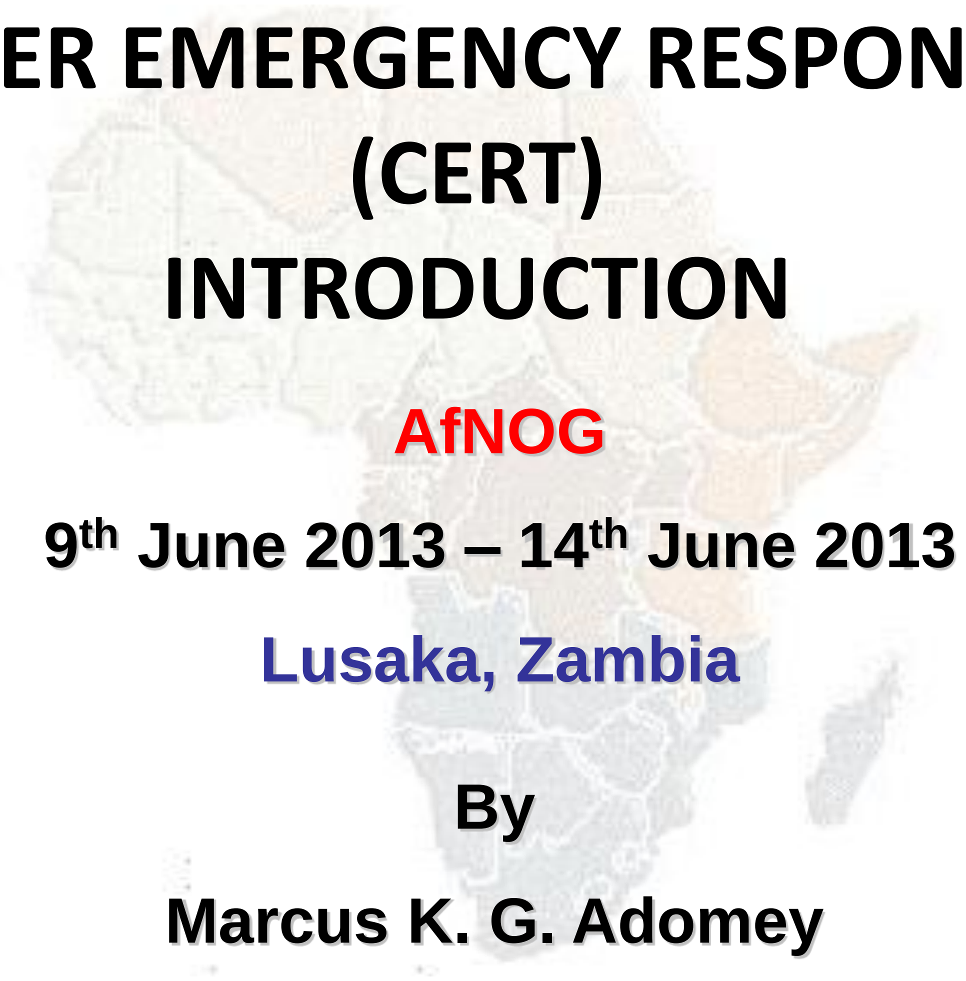
COMPUTER EMERGENCY RESPONSE TEAM (CERT) INTRODUCTION



AfNOG

9th June 2013 – 14th June 2013

Lusaka, Zambia

By

Marcus K. G. Adomey

OUTLINE

- Definition of CERT
- Acronyms of CERT
- Types of CERT
- History of CERT
- CERT in the World
- CERT Services
- CERT Framework
- CERT Organizational Model
- CERT Staff
- CERT Creation

DEFINITION OF CERT

It is an organization or team that provides, to a defined constituency, services and support for both preventing and responding to computer security incidents

ACRONYMS OF CERT

Various acronyms and titles have been given to CERT organizations over the years.

These titles include

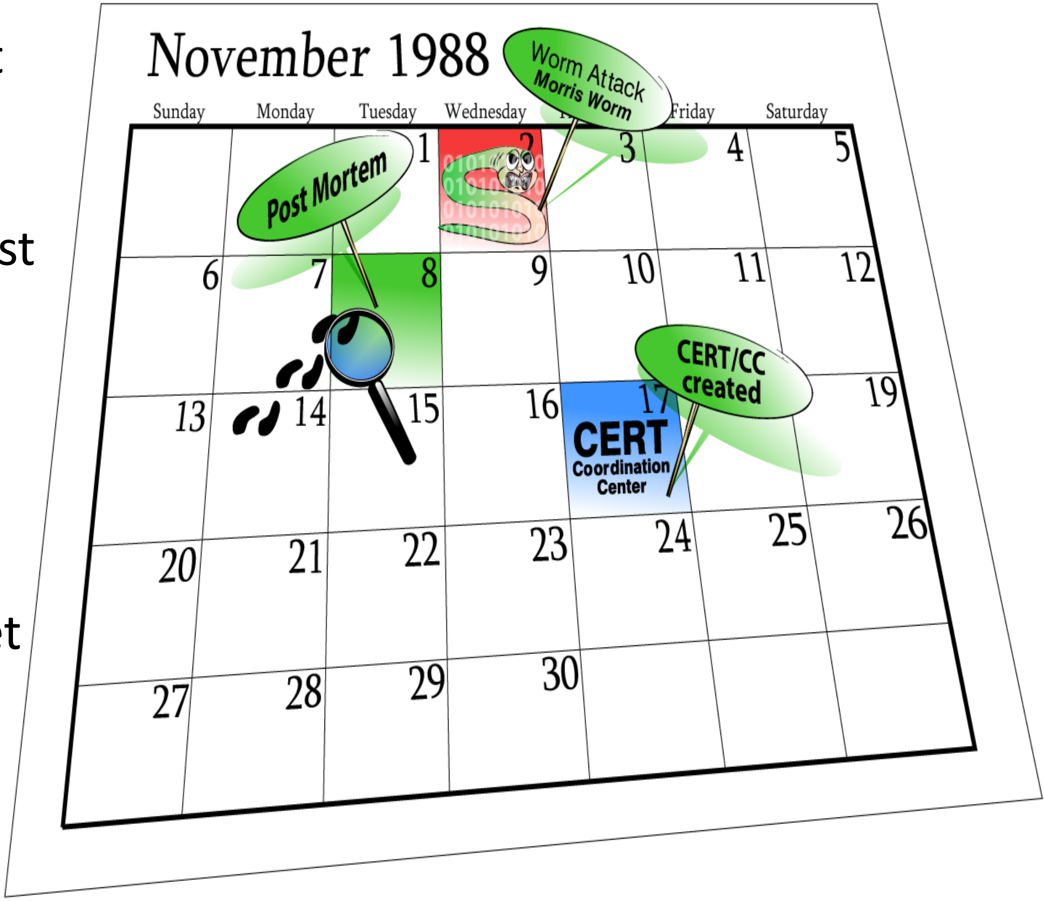
CSIRT	-	Computer Security Incident Response Team
CSIRC	-	Computer Security Incident Response Capability or Center
CIRC	-	Computer Incident Response Capability or Center
CIRT	-	Computer Incident Response Team
IHT	-	Incident Handling Team
IRC	-	Incident Response Center or Incident Response Capability
IRT	-	Incident Response Team
SERT	-	Security Emergency Response Team
SIRT	-	Security Incident Response Team

HISTORY OF CERT

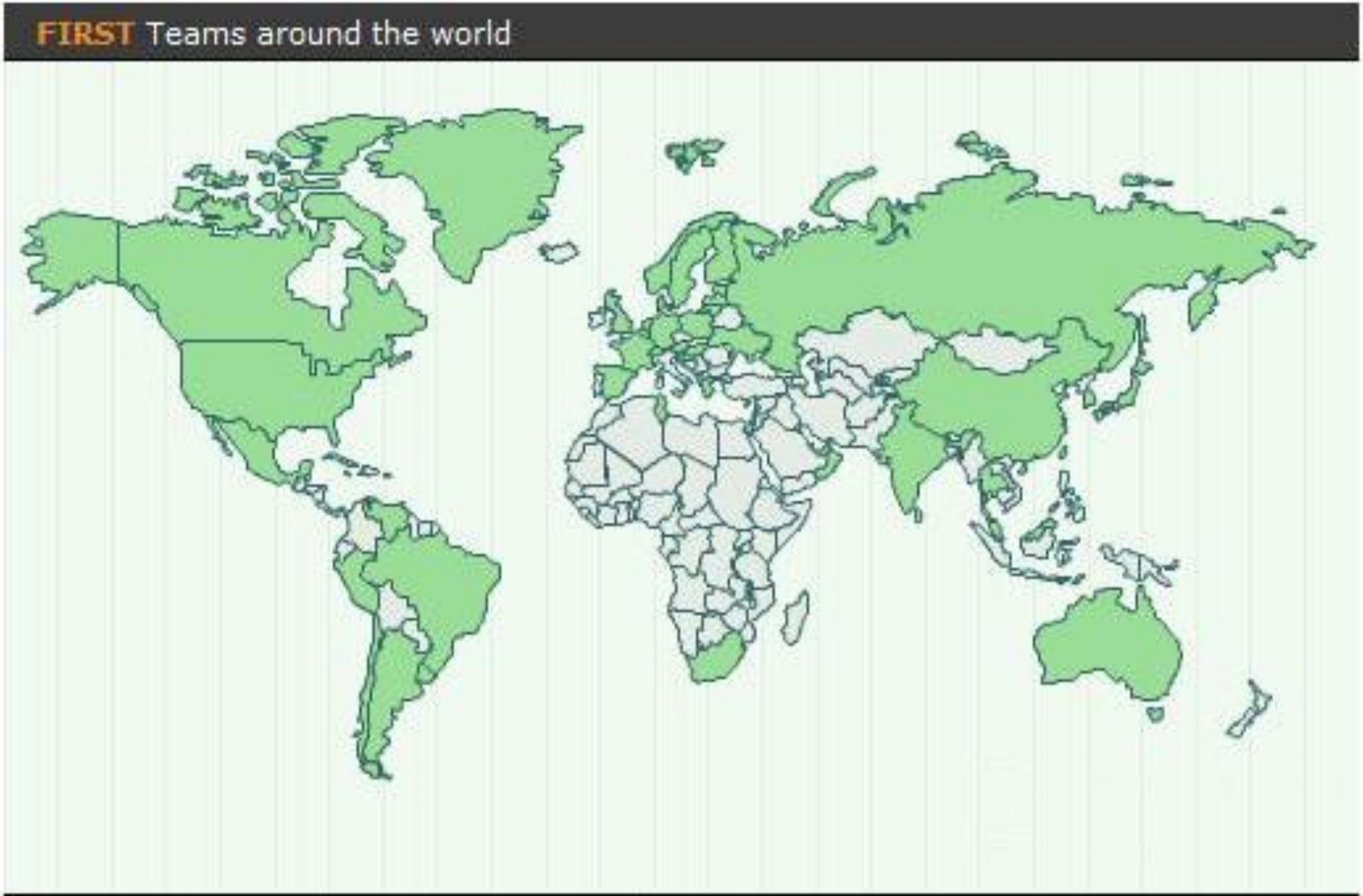
Morris is accompanied by his mother, Anne, left, and his father, Robert Sr., at right rear, after a day of jury selection in his trial on charges of infiltrating a nationwide computer network in Nov. 1988

CERT HISTORY

- ✓ Robert Tappan Morris then student at Cornell University launched on November 2, 1988 from MIT the first and fast self-replicating computer worms via the Internet
- ✓ Crippled almost 10% (6000) of the computer connected to the Internet in Nov 1988.



CERTs IN THE WORLD



CERTs IN THE WORLD

In Africa

AfricaCERT

United in promoting cyber security in Africa

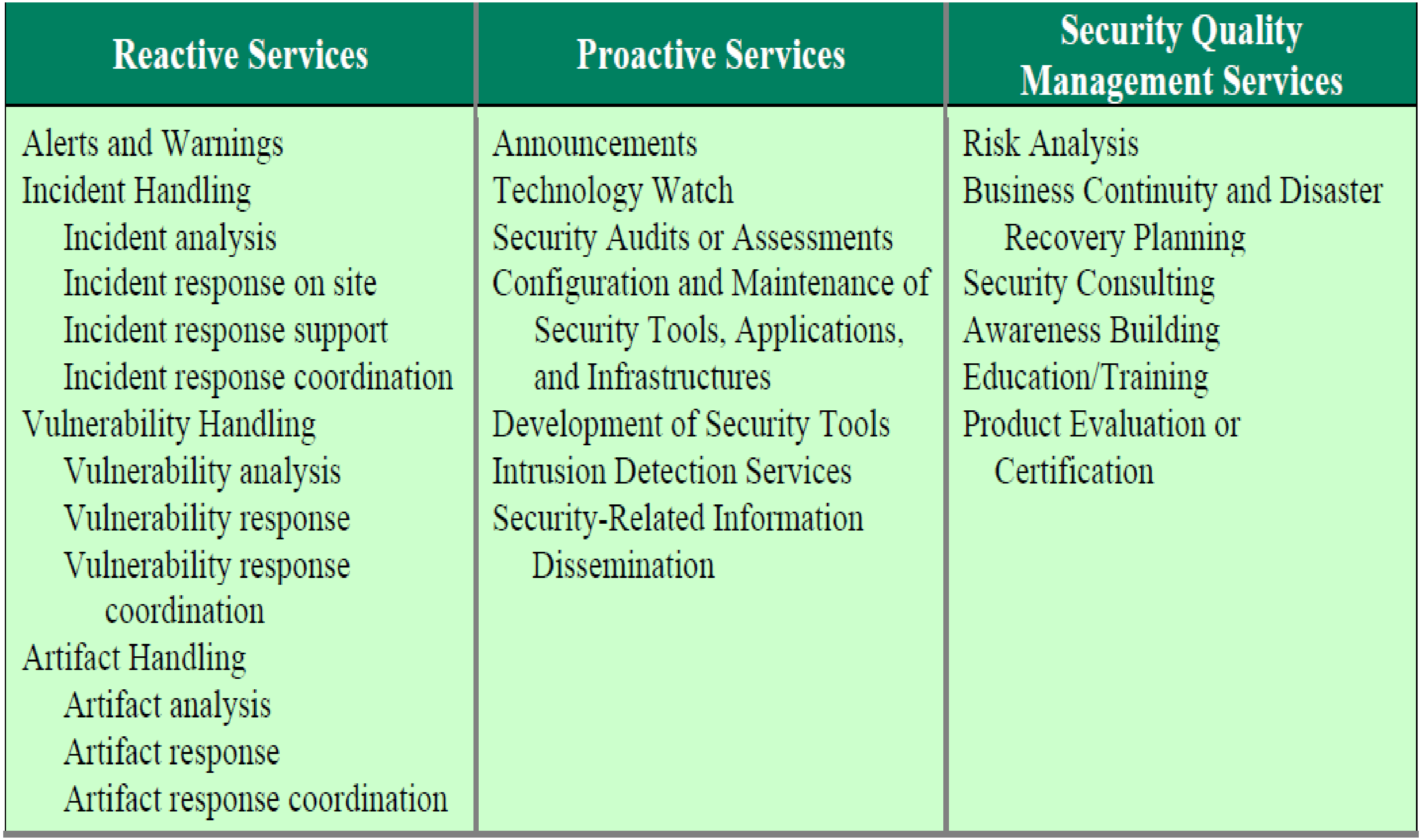
Africa CERT

In Africa, few countries have started their security project and fulfilled some good steps; other countries have now started implementing national mechanisms for combating cybercrime and other related threats; however, a sizeable number of African countries still do not have a strategic plan and are unable to start their first actions.

Africa CERT: The African response to capacity development on cyber security in Kigali, 30th of May 2010

What about your country???

CERT SERVICES



Reactive Services	Proactive Services	Security Quality Management 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	Announcements Technology Watch Security Audits or Assessments Configuration and Maintenance of Security Tools, Applications, and Infrastructures Development of Security Tools Intrusion Detection Services Security-Related Information Dissemination	Risk Analysis Business Continuity and Disaster Recovery Planning Security Consulting Awareness Building Education/Training Product Evaluation or Certification

TYPES OF CERT

There could be some of the following CERT:

- GovCERT
  - Military CERT
  - Police CERT
  - Finance CERT
  - Health CERT
- Academic CERT
- ISP CERT
- Bank CERT
- Industry CERT
- - - - -

CERT FRAMEWORK

- Constituency
- Mission
- Funding and Cost
- CERT Authority
- CERT Organizational Placement
- Policy and procedures
- Models and Legal Basis of Cooperation

CERT FRAMEWORK

Constituency

The constituency is the organization (or group of organizations) and/or people whose incidents CERT handles (or co-ordinates)

There are several different ways for defining constituency. It can be defined by:

- range of IP addresses
- AS (autonomous system) number(s)
- domain name(s)
- free text description
- - - - - - -

CERT FRAMEWORK

CERT Mission

- A mission statement is a statement that defines the essence or purpose of a company or organization. It answers the question, "Why do we exist?“
- Consist of at least three or four sentences used by an organization to explain, in simple and concise terms, their purposes for being.

CERT FRAMEWORK

CERT Mission statement should

- be non-ambiguous
- be imperative to enable the CERT to establish a service and quality framework, including the nature and range of services provided, the definition of its policies and procedures, and the quality of service.

If the team is housed within a large organization or is funded from an external body, the CERT mission statement must complement the mission of those organizations

CERT FRAMEWORK

Example of Mission Statement

SingCERT's Mission Statement:

"One Point of Trusted Contact

Facilitate Security Threats Resolution

Increase National Competency in IT Security"

Fictitious CERT mission statement:

"Fictitious CERT provides information and assistance to the staff of its hosting company to reduce the risks of computer security incidents as well as responding to such incidents when they occur."

Costs and Funding

CERTs are most often funded by a parent organization, whether it is a university, commercial organization, military organization, or government entity.

Question

"How much does it cost to start and operate a CERT?"

There is no one figure that can be given for what a CERT will cost to set up and operate.

The costs for setting up a team depend on the circumstances and environment in which the team is established.

CERT FRAMEWORK

Type of Costs

■ **Start-Up Costs**	■ **Sustainment Costs**
○ Software	○ ongoing facilities maintenance
○ Computing equipment	○ support of equipment upgrades
○ Capital furniture expenditures supplies	○ supplies
○ Internet domain registration fees	○ travel
○ Facilities costs	■ **Personnel Costs**
○ Phones	○ raises
○ Fax machines	○ professional development
■ **Personnel Costs**	○ training
○ salaries	
○ benefits	

CERT Funding Strategies

STRATEGY	DESCRIPTION
Membership subscriptions	Time-based subscription fees for delivery of a range of services
Contract services or fee-based services	Payment for services as delivered
Government sponsorship	A government department funds the CERT
Academic or research sponsorship	A university or research network funds the CERT
Parent organization funding	A parent organization establishes and funds the CERT
Consortium sponsorship	Group of organizations, government entities, universities, etc. pool funding
A combination of the above	For example, funding is provided through government funding and private contract

CERT FRAMEWORK

CERT Authority

There are three levels of authority or relationships that a CERT can have with its constituency

- **Full authority**: The CERT can make decisions, without management approval, to direct response and recovery actions.
- **Shared authority**: The CERT participates in the decision process regarding what actions to take during a computer security incident, but can only influence, not make the decision.
- **No authority**: The CERT cannot make any decisions or take any actions on its own. The CERT can only act as an advisor to an organization, providing suggestions, mitigation strategies, or recommendations.

CERT Organizational Placement

- The place that a CERT holds in its parent organization is tightly coupled to its stated mission, its constituency and to its Organizational model.

- There is no clear standard or consistent placement or location of a CERT within the organizational reporting structure of a host or parent organization.

CERT FRAMEWORK

Policies and Procedures

All services and CERT functions should be supported by well-defined policies and procedures.

A documented set of policies and procedures is vital to

- ✓ ensure that team activities support the CSIRT mission
- ✓ set expectations for confidentiality
- ✓ provide the framework for day-to-day operational needs
- ✓ maintain consistency and reliability of service

CERT FRAMEWORK

Example Policies

- ✓ security policy
- ✓ open reporting environment policy
- ✓ incident reporting policy
- ✓ incident handling policy
- ✓ external communications policy
- ✓ media relations policy
- ✓ information disclosure policy
- ✓ information distribution policy
- ✓ human error policy
- ✓ training and education policy
- ✓ CSIRT acceptable use policy

CERT FRAMEWORK

Example Procedures

- ✓ standard operating procedures (SOPs)
- ✓ accepting and tracking incident reports
- ✓ answering the hotline
- ✓ incident and vulnerability handling
- ✓ gathering, securing, and preserving evidence
- ✓ configuration of CSIRT networks and systems
- ✓ system and network monitoring and intrusion detection
- ✓ backing up and storing incident data
- ✓ notification processes (how information is packaged, distributed, archived, etc.)
- ✓ training and mentoring

CERT FRAMEWORK

Relationship to Other Teams

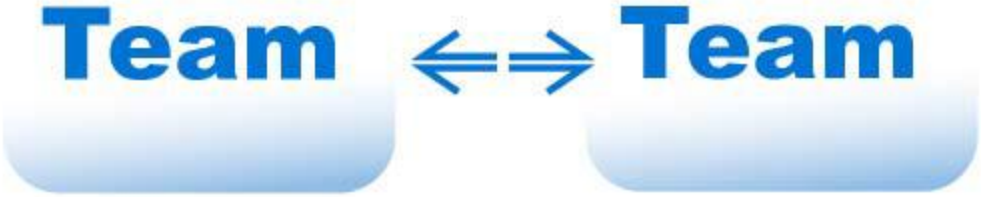
- The realm of CERTs is the Internet, and therefore the world
- There are many constituencies and CERT around the world
- At some level these CERTs have to inter-operate in order to get their job done.
- This cooperation and coordination effort is at the very heart of the CERT framework

CERT FRAMEWORK

Models of cooperation

Bilateral team-team cooperation

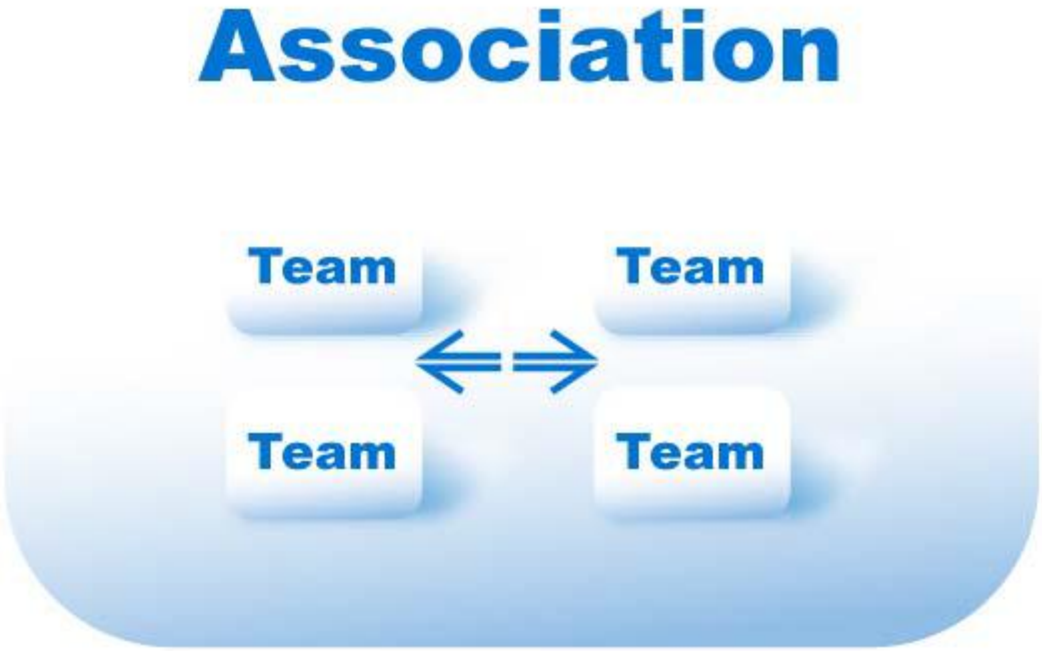
- This is a model of a bilateral cooperation between two teams only.
- It is based on the trust between particular teams and their members, usually built over years, for example through joined participation in security projects.
- This kind of cooperation is often stimulated by common goals for future development and similar team missions.



CERT FRAMEWORK

Models of cooperation

Association



CERT FRAMEWORK

Models of cooperation

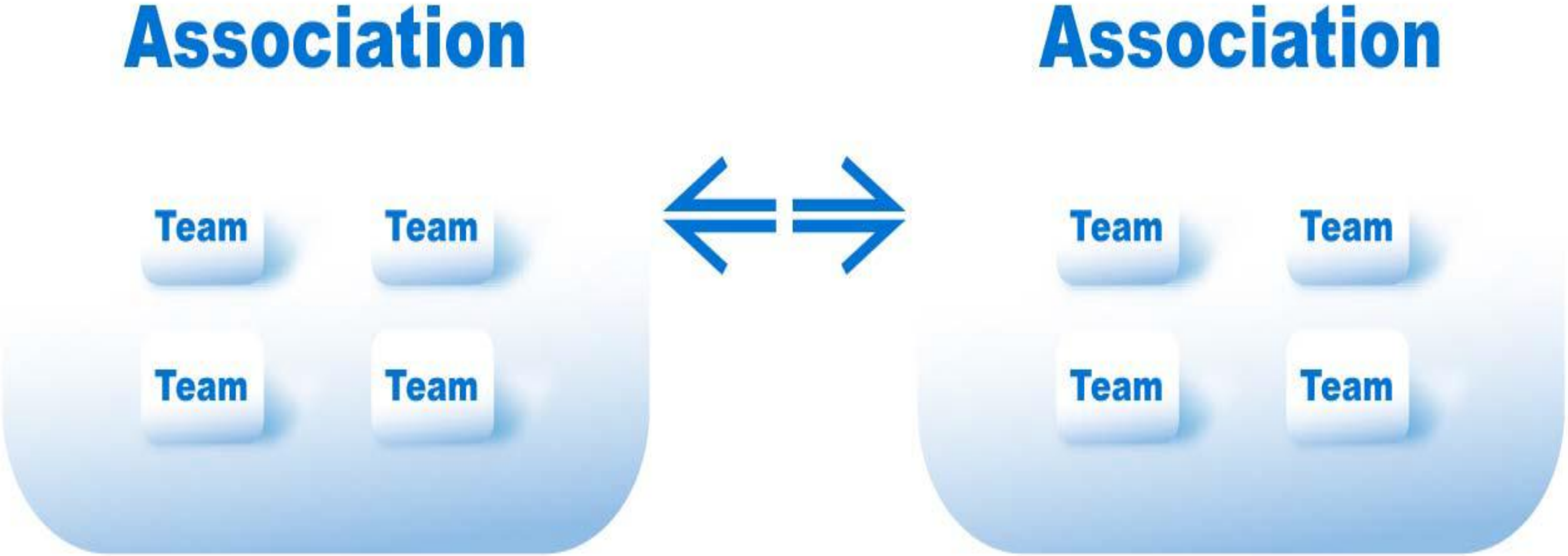
Association

- The association is a model of cooperation between many teams which have common interests and goals.
- The framework for this kind of cooperation might be set by a common geographical area (like in the national cooperation activities), common sets of services, similar constituencies, sector of operations etc.
- The association model comes with different names: forum, taskforce, group, coalition, alliance etc.

CERT FRAMEWORK

Models of cooperation

Cooperation between associations



CERT FRAMEWORK

Models of cooperation

Cooperation between associations

- This model depicts cooperation among two or more associations.
- It is usually based on the common goals of both organisations and shared benefits.
- This kind of cooperation is very often realised by exchanging experiences (for example delegates on the organisation’s meetings) and formulation of common goals and rules of cooperation (for example Memorandum of Understanding)

CERT FRAMEWORK

Legal basis for cooperation

Non-disclosure agreement

- A non-disclosure agreement (NDA), sometimes also called a confidential disclosure agreement (CDA), confidentiality agreement or secrecy agreement, is a legal contract between at least two parties which outlines confidential materials or knowledge the parties wish to share with one another for certain purposes, but wish to restrict from generalized use.
- In other words, it is a contract through which the parties agree not to disclose information covered by the agreement.
- An NDA creates a confidential relationship between the parties to protect any type of trade secret.
- As such, an NDA can protect non-public business information.

Legal basis for cooperation

Memorandum of Understanding

A Memorandum of Understanding (MOU) is a legal document describing a bilateral agreement between parties. It expresses a convergence of will between the parties, indicating an intended common line of action, rather than a legal commitment. It is a more formal alternative to a gentlemen's agreement, but generally lacks the binding power of a contract.

CERT FRAMEWORK

Legal basis for cooperation

Contract

A contract is a "promise" or an "agreement" made of a set of promises. Breach of this contract is recognized by the law and legal remedies can be provided. In civil law, contracts are considered to be part of the general law of obligations. The law generally sees performance of a contract as a duty

CERT FRAMEWORK

Legal basis for cooperation

Terms of Reference

Creating a detailed Terms of Reference is critical to the success of an association, as it defines its purpose of existence:

- ➢ Vision, objectives, scope and deliverables (i.e. what has to be achieved)
- ➢ Stakeholders, roles and responsibilities (i.e. who will take part in it)
- ➢ Resource, financial and quality plans (i.e. how it will be achieved)
- ➢ Work breakdown structure and schedule (i.e. when it will be achieved)

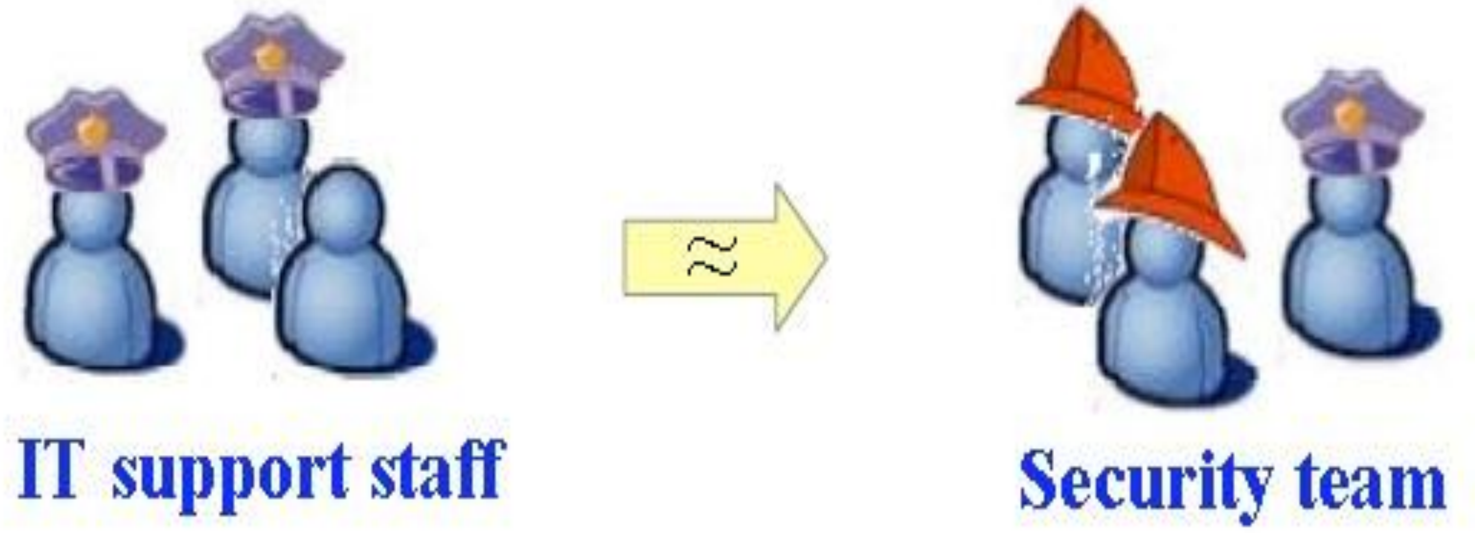
CERT ORGANIZATIONAL MODEL

Organizational Models for CERT

- ❑ Security Team
- ❑ Internal Distributed CERT
- ❑ Internal Centralized CERT
- ❑ Combined Distributed & Centralized CERT
- ❑ Coordinating CERT

CERT ORGANIZATIONAL MODEL

Security Team



CERT ORGANIZATIONAL MODEL

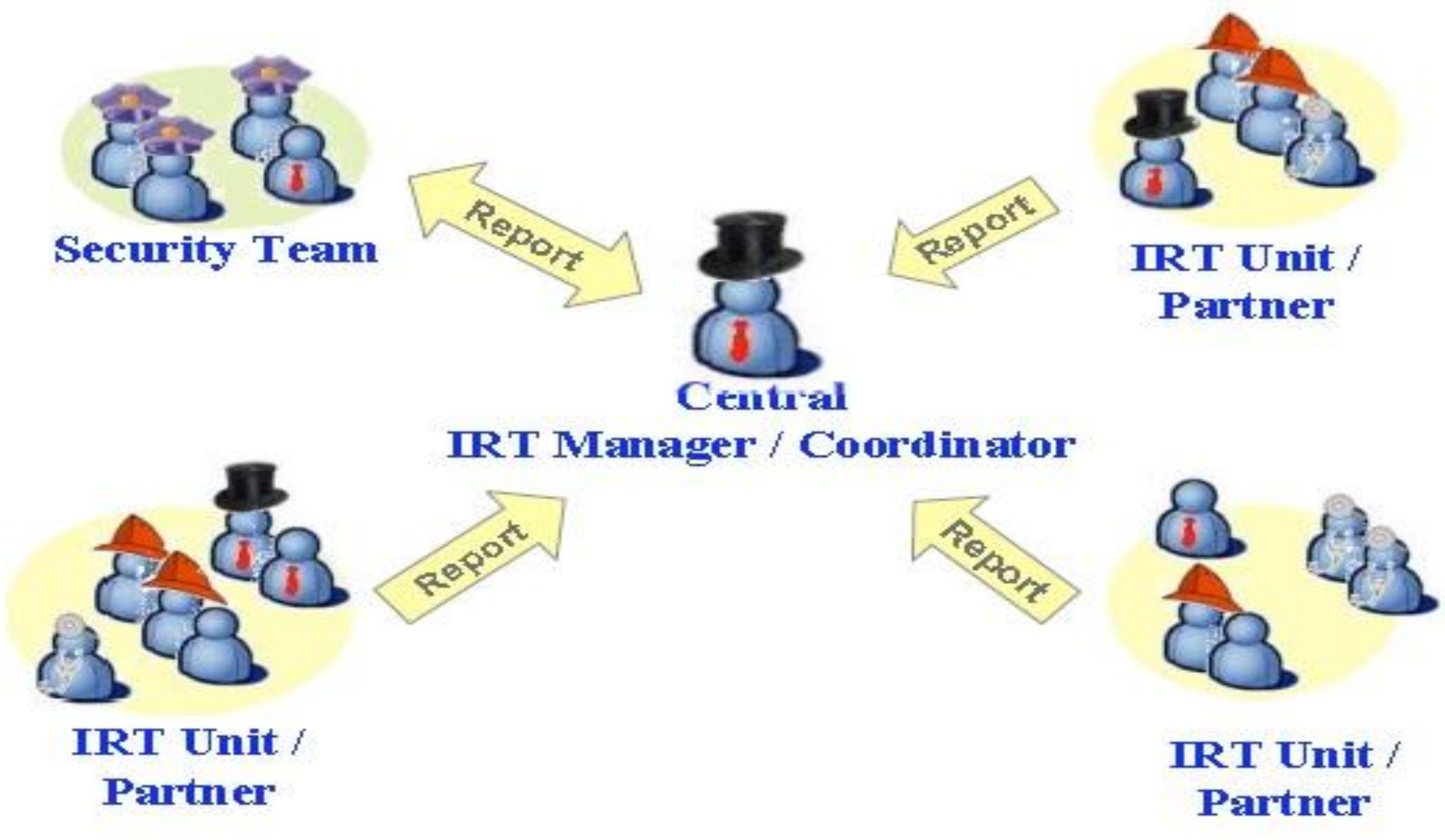
Security Team

In this model

- CSIRT has not been established
- No group or section of the organization has been given the formal responsibility for all incident handling activities
- Incident response efforts are not necessarily coordinated or standardized across the organization
- Network or security administrators at the local or division level handle security events on an ad hoc and sometimes isolated basis as part of their overall responsibilities or job assignments

CERT ORGANIZATIONAL MODEL

Internal Distributed CSIRT



CERT ORGANIZATIONAL MODEL

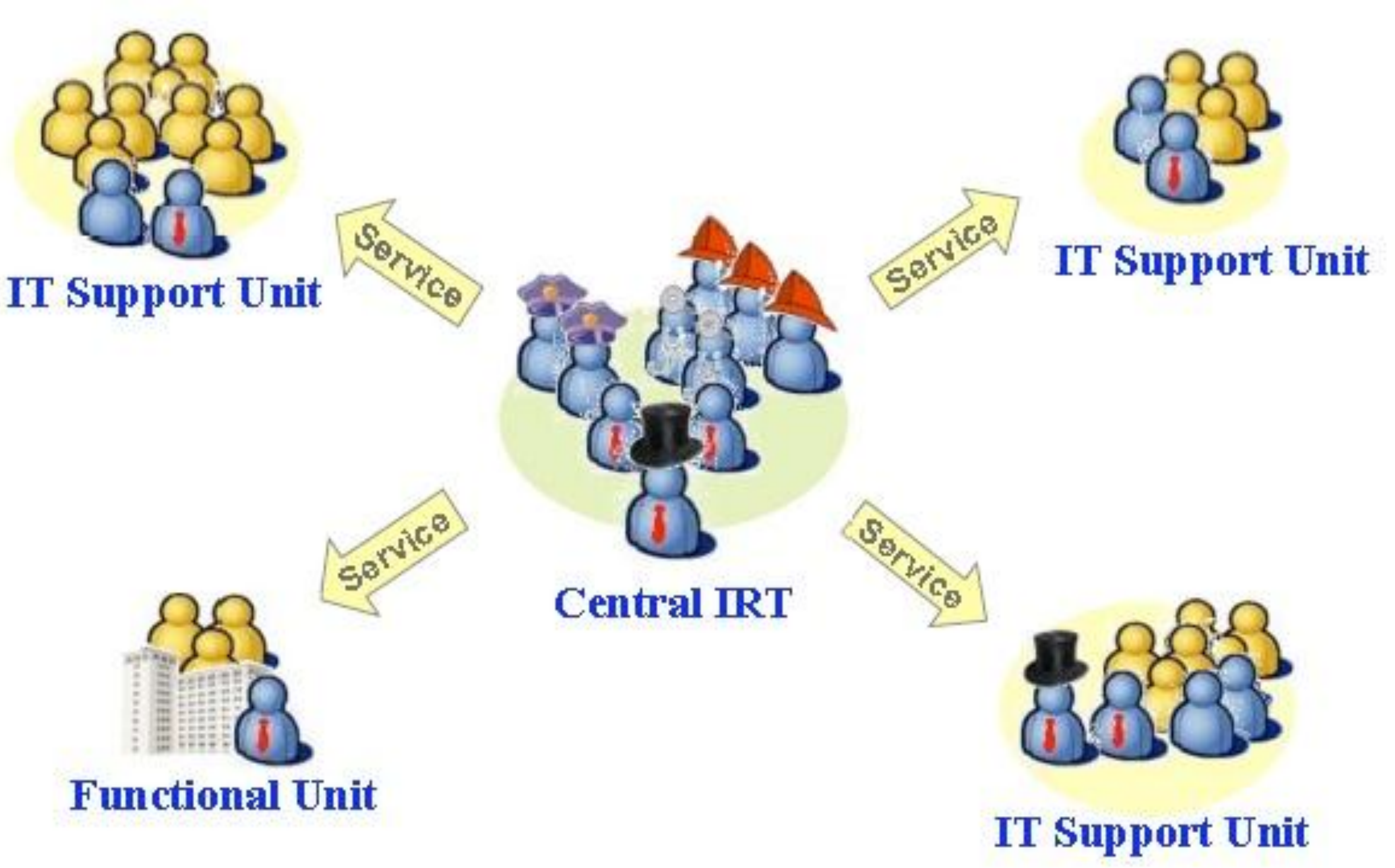
Internal Distributed CSIRT

In this model

- The organization utilizes existing staff to provide a “virtual” distributed CSIRT, which is formally chartered to deal with incident response activities
- The distributed team members can perform CSIRT duties in addition to their regular responsibilities or could be assigned to CSIRT work on a full-time basis
- Across the organization, individuals are identified as the appropriate points of contact for working as part of the distributed team based on their or based on their geographic location or functional responsibilities.
- There is a manager who oversees and coordinates activities for the distributed team.
- The CSIRT serves as the single point of contact into the organization in relation to incident or vulnerability reports or activity for both internal and external parties.

CERT ORGANIZATIONAL MODEL

Internal Centralized CSIRT



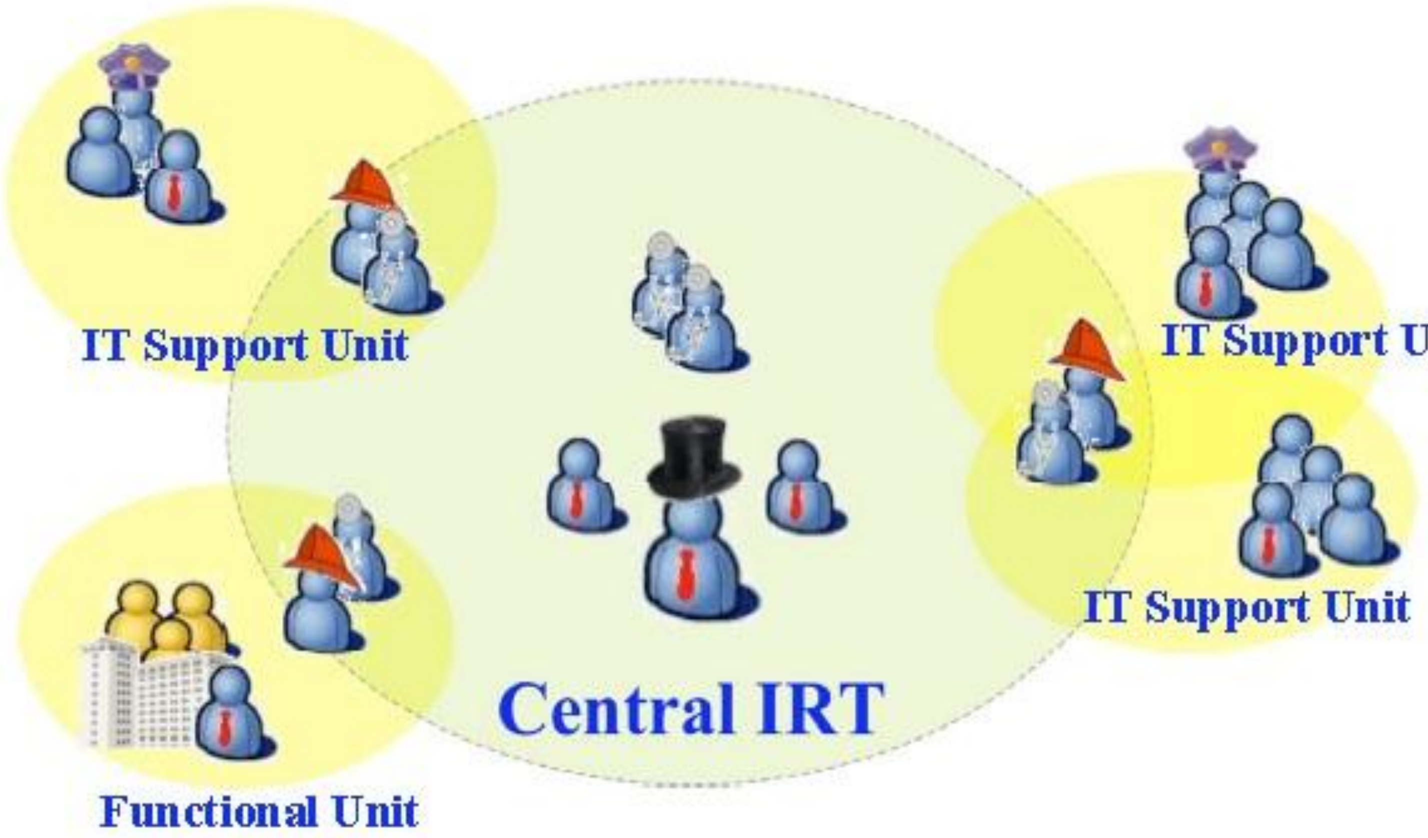
CERT ORGANIZATIONAL MODEL

Internal Centralized CSIRT

- This model is a fully staffed, dedicated CSIRT that provides the incident handling services for an organization.
- In many cases team members spend 100% of their time working for the CSIRT;
- There is a CSIRT manager who reports to high-level management such as a chief information officer (CIO), chief security officer (CSO), or even chief risk officer (CRO) or some other equivalent manager.
- The team is centrally located in the organization and is responsible for all incident handling activities across the constituency or enterprise.
- The CSIRT serves as the single point of contact into the organization in relation to incident or vulnerability reports or activity for both internal and external parties.

CERT ORGANIZATIONAL MODEL

Internal Combined Distributed and Centralized CSIRT



CERT ORGANIZATIONAL MODEL

Internal Combined Distributed and Centralized CSIRT

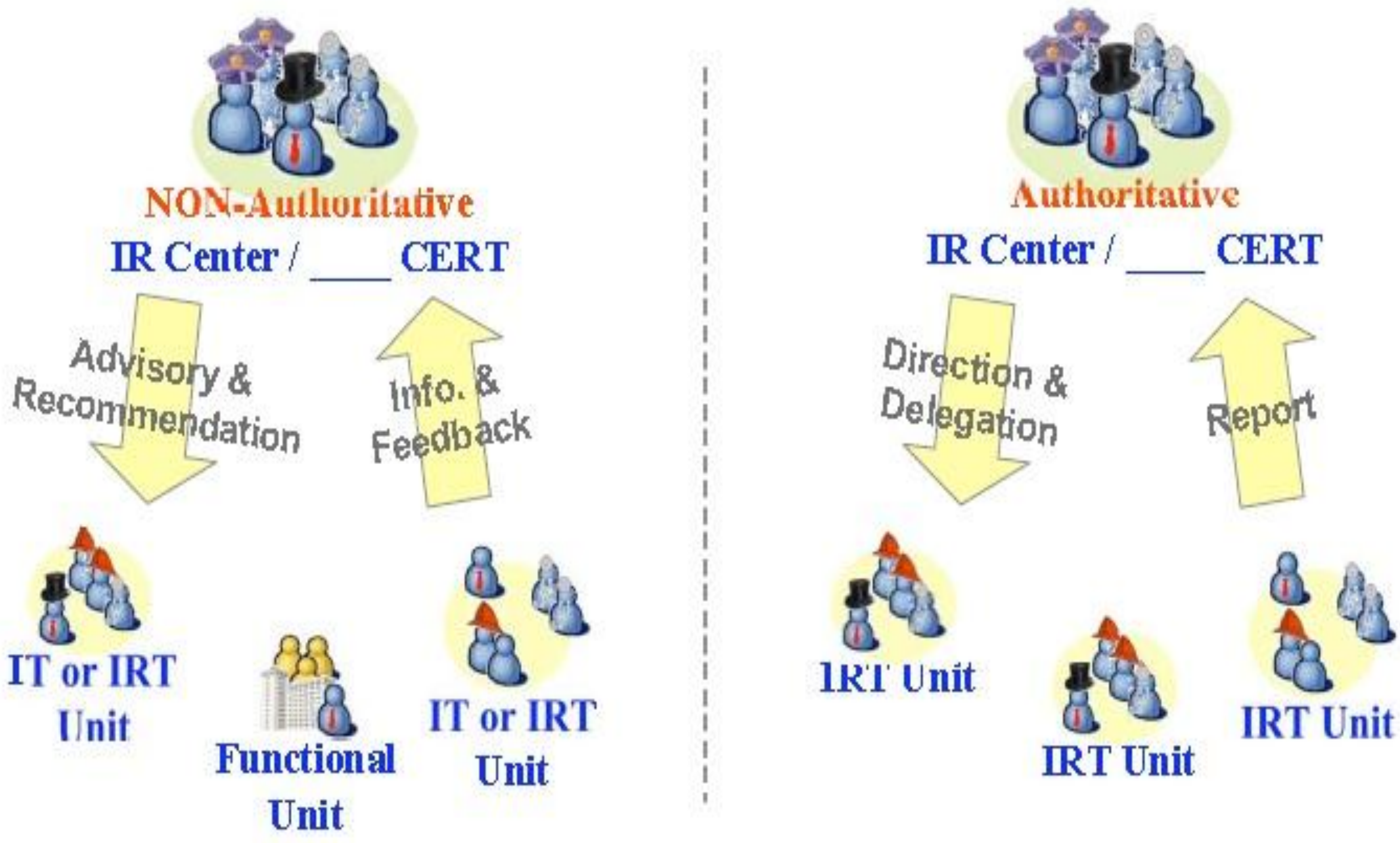
- This model represents a combination of the distributed CSIRT and the centralized CSIRT.

- It maximizes the utilization of existing staff in strategic locations throughout the organization with the centrally located coordinating capabilities of the dedicated team to provide a broader understanding of the security threats and activity affecting the constituency within the enterprise.

- The CSIRT serves as the single point of contact into the organization in relation to incident or vulnerability reports or activity for both internal and external parties.

CERT ORGANIZATIONAL MODEL

Coordinating CERT



CERT ORGANIZATIONAL MODEL

Coordinating CERT

Coordinating CERTs usually have a broader scope and a more diverse constituency.

There are two types:

- Non-authoritative
- Authoritative

Authoritative

Coordinate incident and vulnerability handling activities across organization or governing boundary

Non-authoritative

Facilitate incident and vulnerability handling activities for external constituency

CERT ORGANIZATIONAL MODEL

Examples of Coordinating CERT

Non-authoritative

- FIRST (www.first.org)
- CERT Coordination Center (www.cert.org)
- US CERT (www.us-cert.gov)
- Japan CERT Coordination Center (www.jpcert.or.jp)

Authoritative

- Siemens-CERT (Munich, Germany)
- US NAVCIRT (www.ncdoc.navy.mil)
- NYS CSCIC IRT (www.cscic.ny.us)
- Korea National CERT (www.ncsc.go.kr)

CERT STAFFING

- CERT with capable incident handling needs people with a certain set of personal skills and technical expertise
- The composition of CSIRT staff varies from team to team and depends on a number of factors, such as
  - Mission and goals of the CSIRT
  - Nature and range of services offered
  - Available staff expertise
  - Constituency size and technology base
  - Anticipated incident load
  - Severity or complexity of incident reports
  - Funding

CERT STAFFING

What type of staff will you need?

How will you staff your CSIRT?

Options

- ✓ Hire dedicated CSIRT staff.
- ✓ Use existing staff.
  - ▪ full-time - part-time
  - ▪ rotation - ad hoc
  - ▪ Hire contractors.
- ✓ Outsource.

CERT STAFFING

Types of CSIRT Roles

Core Staff	Extended Staff
✓ manager or team lead ✓ assistant managers, supervisors, or group leaders ✓ hotline, help desk, or triage staff ✓ incident handlers ✓ vulnerability handlers ✓ artifact analysis staff ✓ forensic analysts ✓ platform specialists ✓ Trainers ✓ technology watch	✓ support staff ✓ technical writers ✓ network or system administrators for CSIRT infrastructure ✓ programmers or developers (to build CSIRT tools) ✓ web developers and maintainers ✓ media relations ✓ legal or paralegal staff or liaison ✓ law enforcement staff or liaison ✓ auditors or quality assurance staff ✓ marketing staff

CERT STAFFING

Staff Skills

Personality

- ✓ people skills
- ✓ communication skills

Technical Skills

- ✓ system and network administration experience
- ✓ platform expertise: UNIX/Linux, Windows, Mac
- ✓ basic understanding of Internet protocols
- ✓ programming experience

Security Training

- ✓ incident handling experience
- ✓ problem solving abilities
- ✓ basic understanding of common computer attacks and vulnerabilities

Be aware of

- ✓ any requirements you might have regarding obtaining security clearances
- ✓ the need for service level agreements and data protection agreements with contractors and managed service providers

CERT: to do list

1. **Identify Stakeholders and participants**
2. **Obtain management support and sponsorship**
3. **Develop a CERT project plan**
4. **Gather Information**
5. **Identify the CERT Constituency**
6. **Defined the CERT mission**
7. **Secure funding for CERT operations**
8. **Decide on the range and level of services the CERT will offer**
9. **Determine the CERT reporting structure, authority and organizational model**

CERT: to do list

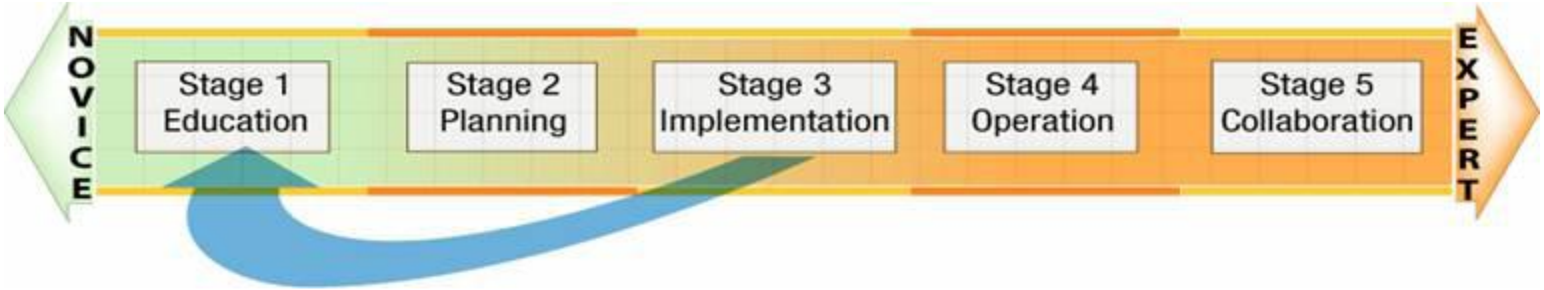
10. Identify required resources such as staff equipment and infrastructure
11. Define interaction and interfaces
12. Define roles responsibilities and the corresponding authority
13. Document the workflow
14. Develop policies and corresponding procedures
15. Create and implementation plan and solicit feedback
16. Announce the CERT when it becomes operational
17. Define methods for evaluating the performance of the CERT
18. Have a backup plan for every element of the CERT

19. BE FLEXIBLE

STEPS FOR CREATING A CSIRT

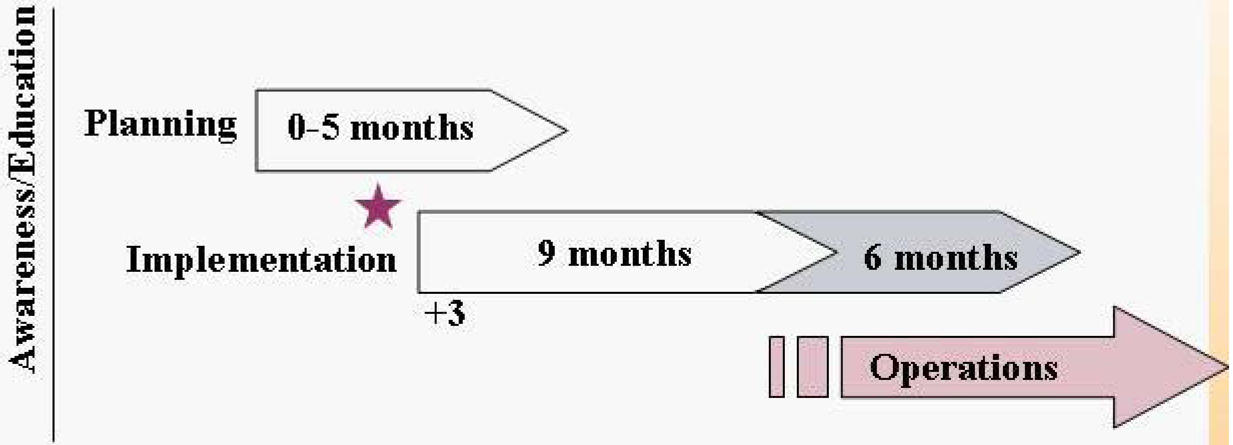
Steps for Creating a CSIRT

- Stage 1 – Educate stakeholders about the development of CERT
- Stage 2 – Plan the CERT
- Stage 3 – Implement the CERT
- Stage 4 – Operate the CERT
- Stage 5 – Collaboration



Timeline

Depending on the resources that are provided and “buy-in” from its key stakeholders and constituency, a CSIRT can take anywhere from 18-24 months to become fully operational (see the projected timeline below). This timeline can be extended or compressed, depending on a number of factors and decision points that are made. These are indicated at the bottom of the picture.



★ Course of Action - Decision points to be considered:

1. mission/vision
2. constituency
3. scope
4. authority
5. services (interaction/levels/structure)
6. external interactions
7. terminology (incidents, types, categories)

QUESTIONS

Thanks!

THE END