Internet Society
Gambia Chapter

PROGRESS PEACE PROSPERITY

AfricaCERT
United in promoting cyber security in Africa

The Role of
Computer Security Incident Response Team (CSIRT)
in our economy

By Marcus K. G. Adomey

OVERVIEW

❑ Cyberspace and the Internet

❑ Cybercrime and Cybersecurity

❑ Computer Security Incident Response Team

❑ Importance of CSIRT in our Economy

❑ Philosophy of CSIRT

Cyberspace and the Internet

Cyberspace and the Internet

What is cyberspace?

Cyberspace should not be confused with the Internet,

Rather the Internet is the basis for cyberspace

Cyberspace and the Internet

What is the Internet?

The Internet

- ❑ is the global interconnected private, public, academic, business, and government networks;
- ❑ uses the Internet protocol suite (TCP/IP) to link several billion devices world wide.

TCP/IP Stack	
APPLICATIONS	Email, TELNET, SSH
INTERNET SERVICES	DNS, DHCP, HTTP,
TCP/IP Protocols Suite	TCP/IP Protocols Suite
HARDWARE	Computers, Mobile Phones Wires, Wireless Satellites

Cyberspace and the Internet

What is cyberspace?

Cyberspace also known as

- ❑ virtual space,
- ❑ non-physical space,
- ❑ online world,
- ❑ virtual location,
- ❑ imaginary place
- ❑ "on the Internet"
- ❑ etc.

is a boundless virtual place created through the use of the **INTERNET** and where **SERVICES** are provided.

Cybercrime and Cybersecurity

Cybercrime and Cybersecurity

Cybercrime, or computer-oriented crime, is a crime that involves a computer and a network. The computer

- **may have been used in the commission of a crime**,

  or

- **may be the target**.

Cybercrime and Cybersecurity

Example of DDoS on Estonia

Bronze Soldier of Tallinn

Cybercrime and Cybersecurity

Denial of Service

Tuuli Aug, an editor of the daily newspaper "Eesti Paevaleht," stated the following:

"I felt the country was under attack by an invisible enemy. . . . It was extremely frightening and uncontrollable because we are used to having Internet all the time and then suddenly it wasn't around anymore, . . . You couldn't get information; you couldn't do your job. You couldn't reach the bank; you couldn't check the bus schedule anymore. It was just confusing and frightening, but we didn't realize it was a war because nobody had seen anything like that before“.

Cybercrime and Cybersecurity

Example of Stuxnet in 2010

Nuclear Plant in Iran

Cybercrime and Cybersecurity

Commonwealth Bank ATM Case, Australia

- Commonwealth Bank, Australia - March 2011:- Automatic teller machines (ATMs) spat out tens of thousands of free dollars in Sydney
- IT Security Experts believe that it is the consequence of hacking.

Cybercrime and Cybersecurity

Inappropriate Usage

Cybercrime and Cybersecurity

Shoulder Surfing

Cybercrime and Cybersecurity

Inappropriate Usage

Inappropriate or unacceptable usage refers to person who violates acceptable Information Technology use policies of their organization.

Social Engineering

- Phishing
- Email spamming
- Baiting
- Vishing
- Smishing

- Water-Holing
- Quid Pro Quo
- Tailgating/Peggyback
- Pretexting
- Unwarranted surveillance

- Cyberbullying
- Child Pornography
- Cyberstalking
- Identity Theft
- Scamming

- Transaction Fraud
- Advance Fee Fraud
- Impersonation
- Reverse Social Engineering

Cybercrime and Cybersecurity

There is no clear cut definition

Security is a process, not an end state.

Cybercrime and Cybersecurity

Security/Cybersecurity Features

Security/Cybersecurity is generally defined based on the Triad CIA

- Confidentiality
- Integrity
- Availability

INTEGRITY
CIA TRIAD
AVAILABILITY
CONFIDENTIALITY

Cybercrime and Cybersecurity

Solution

Computer security incidents

- do not respect geographical, timezone, or administrative boundaries in the global Internet.
- is becoming more and more complex and sophisticated
- involves many sites, which may be located in various places around the world and which solution requires collaboration.

One of the solutions to this Internet/Cybersecurity issues is the creation and managing Computer Security Incident Response Team (CSIRT)

What is a
Computer Security Incident Response Team?
(CSIRT)

CSIRT - Definition

Computer Security Incident Response Team

Definition of CSIRT

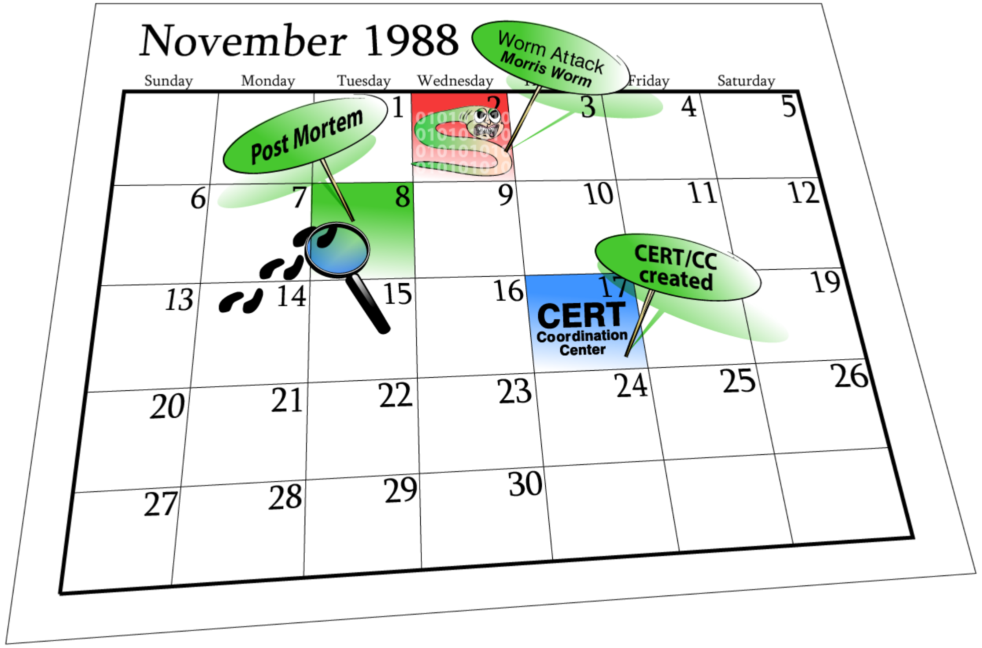
It is an organization that provides, to a defined constituency, services and support for both preventing and responding to computer security incidents.

- Constituency,
- Services and Support
  - Responding
  - Preventing

Computer Security Incident Response Team

CSIRT: History

Computer Security Incident Response Team



- ❑ 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.

CSIRT Functional Framework

CSIRT Functional Framework

Constituency

Computer Security Incident Response Team

CSIRT Constituency

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

There are several different ways for defining constituency.

There could be some of the following CSIRT:

- GovCSIRT
    - Finance CSIRT
    - Health CSIRT
- Military CSRIT
- Police CSRIT
- NatSec CSRIT
- Immigration CSIRT
- Academic CSIRT
- ISP CSIRT
- Bank CSIRT
- Industry CSIRT

Computer Security Incident Response Team

CSIRT - Types

- ❑ Regional
- ❑ National
- ❑ Sectoral
- ❑ Organizational
- ❑ Vendor
- ❑ Commercial

Computer Security Incident Response Team

Every organization must have their CSIRT to protect their critical Assets connected to the Internet

- ❑ Each bank must have its Banks
- ❑ Academic institutions much have their CSIRT
- ❑ Police must have their CSIRT
- ❑ Military must have their CSIRT
- ❑ National Security must have their CSIRT

CSIRT Services

Computer Security Incident Response Team

CSIRT Services

A service is a set of recognizable, coherent functions oriented towards a specific result. Such results may be expected or required by constituents or on behalf of or for the stakeholder of an entity.

A service is specified by the following template:

- ❑ A “Description” field describing the nature of the service.
- ❑ A “Purpose” field describing the intent of the service.
- ❑ An “Outcome” field describing any measurable results of the service.

Computer Security Incident Response Team

CSIRT Services

Reactive Services	Proactive Services	Security Quality Management Services
□ Alerts and Warnings □ Incident Handling □ Vulnerability Handling □ Artifact Handling	□ 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	□ Risk Analysis □ Business Continuity & Disaster Recovery Planning □ Security Consulting □ Awareness Building □ Education/Training □ Product Evaluation or Certification

Beware of the “R” in CSIRT

CSIRT Functional Framework

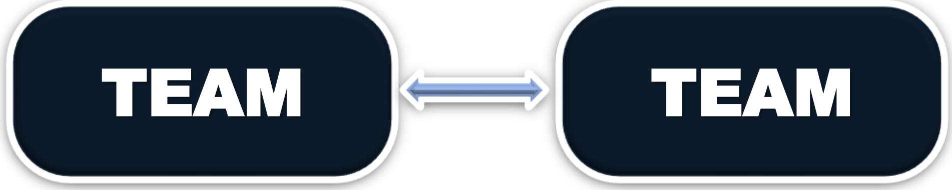
- Mission
- Tools
- Policy and procedures
- CSIRT Authority
- CERT Organizational Placement
- CSIRT Staff
- Funding and Cost

CSIRT Models of Cooperation

CSIRT 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.

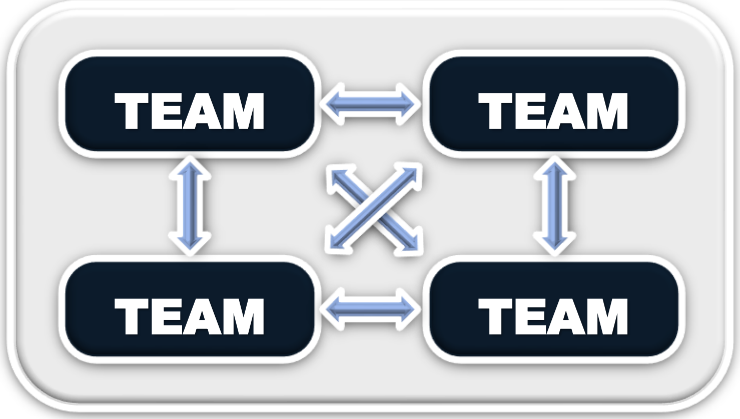

TEAM

TEAM

CSIRT 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.

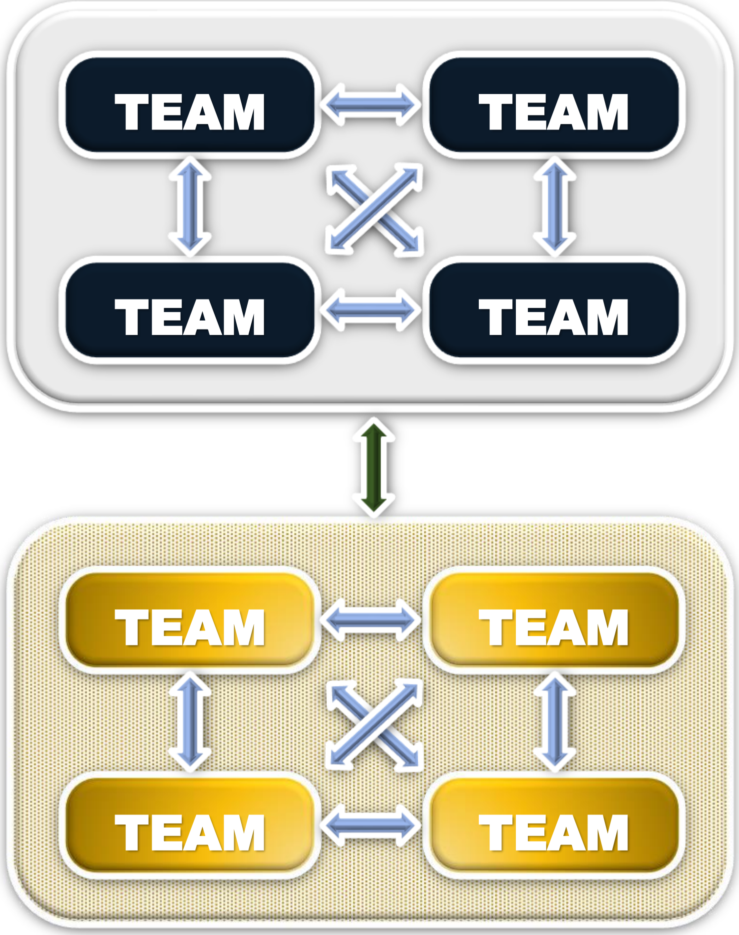


CSIRT Models of Cooperation

Cooperation between associations

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

Example of associations – AfricaCERT and FIRST



CSIRT Models of Cooperation

AfricaCERT

AfricaCERT is the Forum of Computer Security Incident Response Teams and alike organisations covering the Africa Service Regional as defined by AfriNIC.

AfricaCERT fosters cooperation and coordination among Incident Response Teams, promote information sharing.

AfricaCERT provides the following services:

CSIRT Models of Cooperation

AfricaCERT

- ❑ Capacity building to ensure incident response capability thought awareness creation, education and technical trainings.
- ❑ Enabling a community of Security Professionals, Incident Responders, CSIRTs, in Africa that work together in a trusted forum but also. collaborate with others a global level.
- ❑ Ensure access to knowledge, tools and standards.
- ❑ Opening and maintaining dialogue with other stakeholders in the ecosystem which work affect Incident Response Community especially policy makers.

CSIRT Models of Cooperation

Forum Of Incident Response and Security Teams

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

- ❑ FIRST provides a forum for facilitating trusted interactions among incident response and security teams.
- ❑ FIRST hosts an annual Conference on Computer Security Incident Handling.
- ❑ FIRST Technical Colloquia provide a discussion forum for FIRST member teams to share information about vulnerabilities, incidents, tools and all other issues that affect the operation of incident response and security teams.

CSIRT Models of Cooperation

Forum Of Incident Response and Security Teams

- ❑ FIRST members benefit from a variety of technical tools and collaboration channels that enable them to more effectively understand and respond to security incidents.
- ❑ New incident response and security teams can benefit from membership to FIRST by improving communication with peer teams, and exchanging ideas and practices.
- ❑ The collection of teams which compose FIRST provides expertise covering a wide variety of incident response and security issues.

Legal basis for cooperation

- ❑ Memorandum of Understanding
- ❑ Contract
- ❑ Terms of Reference
- ❑ Non-Disclosure Agreement

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.

Legal basis for cooperation

Non-disclosure agreement

The implementation of NDA is done through

❑ the respect of traffic light protocol and

❑ the use encryption

Legal basis for cooperation

Traffic Light Protocol

The Traffic Light Protocol (TLP)

- is a set of designations used to ensure that sensitive information is shared with the appropriate audience
- was created in order to facilitate greater sharing of information
- employs four colors to indicate expected sharing boundaries to be applied by the recipient(s) has four colors; any designations not listed in this standard are not considered valid by FIRST

Legal basis for cooperation

Traffic Light Protocol

🔴 Not for disclosure, restricted to participants only

🟡 Limited disclosure, restricted to participants’ organizations.

🟢 Limited disclosure, restricted to the community.

⚪ Disclosure is not limited.

Legal basis for cooperation

Encryption

❑ The use of GPG/Win4PG

❑ Digital Signature

❑ Key signing party

❑ Web of Trust

Importance of CSIRT in our Economy

Importance of CSIRT in our Economy

The benefits of having having CSIRT in our economy are as follow.

- ❑ Centralized coordination for security incident handling within the organization (Point of Contact, PoC)
- ❑ Minimize and control the damage from computer security incidents
- ❑ Restore operations after incident
- ❑ Fix vulnerabilities quickly and thoroughly
- ❑ Provide guidance for recovery activities
- ❑ Work to prevent incidents from happening in the future

Importance of CSIRT in our Economy

- ❑ Strengthen security to avoid future incidents
- ❑ Dealing with legal issues and preserving evidence in the event of a lawsuit
- ❑ Protect the reputation of the organization.
- ❑ Keeping track of developments in the security field.
- ❑ Ability to bring together a team of experts to analyze and solve complex incident issues

Importance of CSIRT in our Economy

Cybersecurity incidents cost organizations

- ❑ time,
- ❑ money and
- ❑ confidence and reputation.

The longer any incidents go unresolved, the more extensive damage to the organization.

Importance of CSIRT in our Economy

The global cybercrime costs in 2015 is $3 trillion USD

Cybercrime To Cost The World $10.5 Trillion Annually By 2025

Cybercrime Magazine

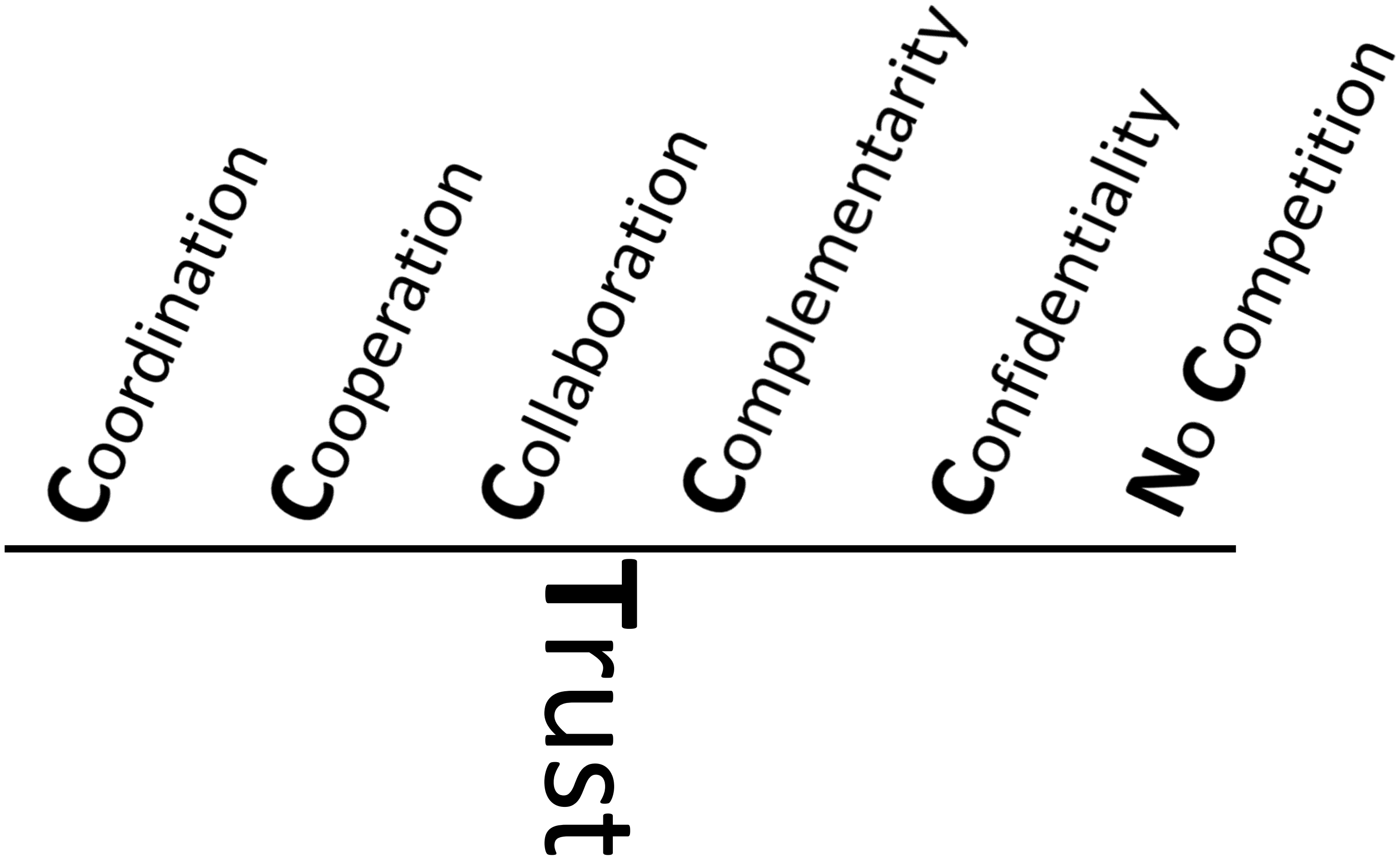
https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

The global cost of cybercrime per minute to reach $11.4 million by 2021

Help Net Security

Philosophy of 5 “C”, “C” barre over “T”

$$\frac{5C\overline{C}}{T}$$



Coordination

Cooperation

Collaboration

Complementarity

Confidentiality

No Competition

Trust

Thanks for your attention

Questions