# CSIRT Staff and Staffing

October 10 – 12, 2016 - Republic of Guinee

By

Marcus K. G. Adomey

# OVERVIEW

CSIRT Staffing

CSIRT Cost and Funding

CSIRT Operation

# CSIRT Staffing

# CERT STAFFING

What type of staff does CSIRT need?

# CSIRT STAFFING

## Types of CSIRT Roles

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

# CSIRT STAFFING

## CSIRT Staff Composition

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

# CSIRT STAFFING

## Staff Skills – Basic

Personality

- people skills
- communication skills
    - Written Communication
        - responses in email concerning incidents
        - documentation of event or incident reports, vulnerabilities, and other technical information
        - notifications and/or guidelines that are provided to the constituency
        - internal development of CSIRT policies and procedures
        - other external communications to staff, management, or other relevant parties
    - Oral Communication

# CSIRT STAFFING

## Staff Skills – Basic

- communication skills
  - Oral Communication

    The ability to communicate effectively though spoken communication is also an important skill to ensure that CSIRT staff members can say the right words to the right people.

    - CSIRT team members
    - system and network administrators (or other IT staff)
    - application owners/developers
    - members of other response teams
    - constituents or users (of the systems)
    - subject matter or technical experts
    - security officers
    - management or other administrative staff
    - human resources staff
    - law enforcement or legal staff
    - press/media/public relations staff
    - vendors

# CSIRT STAFFING

## Staff Skills – Basic

- Presentation Skills
- Diplomacy
- Ability to Follow Policies and Procedures
- Team Skills
- Integrity
- Knowing One's Limits
- Coping with Stress
- Problem Solving
- Time Management

# CSIRT STAFFING

## Staff Skills

### Technical Skills

- Security Features - Confidentiality, Integrity and Availability
- Security Threats and Vulnerabilities/Weaknesses
- The Internet - History, philosophy, and structure and the infrastructures.
- Risks Analysis
- Understanding of Network Protocols
- Network Applications and Services
- system and network administration experience
- Programming Skills

# CSIRT STAFFING

## Staff Skills

### Incident Handling Skills

- Local Team Policies and Procedures
- Understanding/Identifying Intruder Techniques
- Incident Analysis
- Maintenance of Incident Records

# CSIRT STAFFING

## Hiring Staff

How will you staff your CSIRT?

Options

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

# CSIRT STAFFING

## Hiring Staff

Every CSIRT will be bound to specific requirements based on the requirements of their parent organization, local and national laws, and culture.

- pre-interview document check
- pre-interview telephone screening
- reference checks, including criminal records, as appropriate
- interviews that cover topics from Communication Skills technical abilities to social skills and team fit

# CSIRT STAFFING

## Arrival and Exit Procedures

New staff members might be expected to sign CSIRT-specific agreements in addition to any standard employee agreements (such as non-disclosures or intellectual property rights) required by the parent organization.

Exit procedures might include

- change of passwords (both personal and system passwords)
- return of any physical security devices and other media (telephone, pagers, backups)
- revocation of keys (both physical and digital)
- debriefing to review her/his past experiences and to collect ideas for improvements
- exit interview to remind the departing person of responsibilities, which may include additional agreement signing
- an announcement to the constituency and other parties with which the CSIRT regularly interacts
- action to be taken with future correspondence (email, postal) addressed to the individual

# CSIRT STAFFING

## Training Staff

Staff training is necessary from three perspectives:

- bringing new staff members up to the necessary skill level to undertake their work;
- broadening the abilities of existing staff members for personal development and overall team benefit;
- and keeping the overall CSIRT skill set up-to-date with emerging technologies and intruder trends.

# CSIRT STAFFING

## Training Staff

Training should include coverage of the following issues:

- new technical developments
- local team policies and procedures
- understanding and identifying intruder techniques
- communicating with sites
- incident analysis
- maintenance of incident records
- team building
- work load distribution and organizational techniques

# CSIRT STAFFING

## Retaining Staff

- The two main reasons for turnover of CSIRT staff are burnout and low salary
- Meanwhile experienced CSIRT staff are in short supply and expensive to hire and train for your CSIRT environment, so it is most important to try to retain them.

The following approaches should be considered to address both of these issues:

- rotation of duties related to routine work and incident handling
- no more than 80% of any individual’s effort dedicated to incident handling service
- attendance at technical conferences/workshops/tutorials (such as the AfricaCERT Technical training, ITU CyberDrill FIRST Conference)
- participation at technical working groups (like the IETF)
- development of in-house training courses
- attendance at in-house training courses

# CSIRT STAFFING

## Extension of Staff

❑ A CSIRT may be unable to find, fund, train, or hire appropriate staff to provide the necessary specialist skills required by the team.

❑ In such cases, the CSIRT can consider developing relationships with experts in the field to provide the necessary skills.

❑ This will enable the team to cope when the incident load peaks above given thresholds, or in other circumstances defined in the team's escalation policies and procedures.

These additional staffing resources might be drawn from

- other areas of the security teams in the CSIRT parent organization
- other groups in the CSIRT parent organization
- other groups in the CSIRT's constituency
- other CSIRT organizations
- external trusted experts and service providers

# CSIRT STAFFING

## Extension of Staff

- When considering staff to serve in this role, the same hiring principles should apply for them as for any CSIRT member.
- The following processes should be established in advance so extension staff can be activated as quickly as possible:
  - agreed-on criteria for calling in extension staff participation
  - non-disclosure agreements, service level agreements, memoranda of understanding, etc.
  - up-to-date contact information
  - prior agreements from management
  - procedures to establish secure communications
  - initial and regular training

# CSIRT Cost and Funding

# CSIRT - Cost and Funding

**Question** : **“How much does it cost to start and operate a CSIRT?”**

**Answer** : ***There is no one figure that can be given for what a CSIRT 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.***

# CSIRT - Cost and Funding

## 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 | |

# CSIRT - Cost and Funding

## CSIRT 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 |

# CSIRT Operation

# CSIRT Operation

## Operational Elements

- Work Schedules
- Telecommunications
- Email
- Workflow Management Tools (RTIR)
- World Wide Web Information System
- IP Addresses and Domain Name

# CSIRT Operation

## Fundamental Policies

- Code of Conduct
- Information Categorization Policy
- Information Disclosure Policy
- Media Policy - (Establishing a List of Media Contacts - Providing Rules of Engagement - Briefing the Media in Advance - Specifying Out-of-Habitat Behavior - Providing Outreach Through Announcements)
- Security Policy
- Human Error Policy

Thank
you