


Module 1

CSIRT Fundamentals

[Presenter Name]

[Date]



Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

What This Course Is About

Welcome as we gather together to improve the future of security and share our ideas, projects, and successes!

During this course, you will learn to:

- Improve your Computer Security Incident Response Team (CSIRT) processes and procedures
- Deliver prompt and effective resolutions to computer security incidents
- Discuss incidents and causes of problems



Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

Agenda

By the end of this module, you will be able to:

- Define incident management and establish the need for an incident handling team
- Step through potential CSIRT requirements and define how a CSIRT functions
- Define the range, levels of services, and organizational components of a CSIRT
- Set expectations for meeting the needs of constituencies and stakeholders
- Define expectations for a newly created CSIRT and categorize roles and responsibilities
- Set expectations for funding, staffing, and training
- Clarify hardware and software requirements
- Explain how to develop security configurations, including for physical security
- Practice assessing needs for a CSIRT


Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

Section 1:
Why CSIRTs
Are Needed

Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

What Is an Incident?


- **Incident:** Unplanned interruption or quality reduction in IT service
- **Computer security incident:** Compromise or violation of security, a breach of:
 - Confidentiality
 - Integrity
 - Availability



Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

What Is Incident Management?

- **Incident Management (IM):** Process to handle life cycle of an incident
 - Detect and identify
 - Triage and analyze
 - Resolve, including prevent reoccurrence



Goal: Recover quickly to normal operations

Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

CSIRT: Dedicated IM Team

- CSIRT:** Computer Security Incident Response Team
- Supports defined constituency
 - Provides services and support throughout incident life cycles
 - Requires multitasking and organizational skills
 - Custom implementation:
 - Structure and staffing
 - Services provided
 - Policies and procedures
 - PSIRTs focus on product fixes



Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

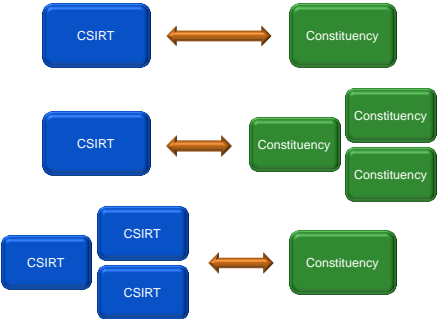
Consider a Separate CSIRT Department

Questions to ask to determine whether a specialized CSIRT is needed outside of the IT department:

- ✓ What needs does the constituency have?
- ✓ What are the critical assets that must be protected?
- ✓ What types of incidents are frequently reported?
- ✓ What computer security problems exist?
- ✓ What type of response is needed?
- ✓ What assistance and expertise is needed?
- ✓ What is the current advanced warning/vulnerability notification setup?
- ✓ Which processes are required?
- ✓ Who will perform what role?
- ✓ Is anyone currently performing that role?

Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

CSIRT Constituency Makeup Varies



Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

Learning Check

What are some advantages and disadvantages of a CSIRT serving more than one constituency?



Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

Questions?

What questions do you have about this lesson?



Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

Section 2:
CSIRT Business Plan

Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

Scope of Responsibility and Services

Work with management or executive sponsor to define and document:

- Span of constituency
- Range of appliances and applications
- Incident management services
 - Onsite incident response
 - Incident response support
 - Incident response coordination



Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

Positioning a CSIRT Organizationally

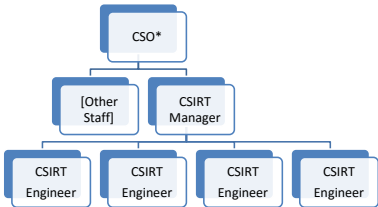
A CSIRT must be appropriately positioned within the organization's business structure

- Within the Chief Security Officer's (CSO's) direct chain of command
- Accountability, visibility, and clout



Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

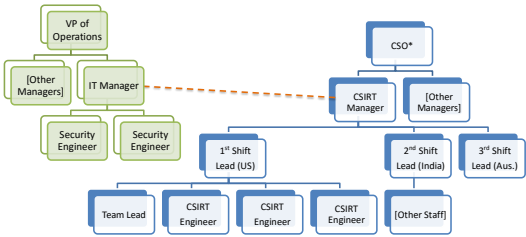
CSIRTs Require Various Roles



* Organization's Chief Security Officer

Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

CSIRTs Require Various Roles



* Organization's Chief Security Officer

Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

CSIRT Mission Statement

Sets ground rules for how CSIRT will operate

- Services Provided
- Policies
- Quality



Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

Each CSIRT Defines Services Provided

- Reactive services
 - Constituency-observed anomalies
 - Automatically-generated alerts and warnings
 - Subsequent incident management
- Proactive services
 - Analysis of constituency practices
 - Actions to improve the security posture
 - Communications such as security bulletins and best practices guidelines
- Quality management services
 - Risk analysis and management
 - Disaster recovery and business continuity
 - Constituency education and training

Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

Creating a Business Plan

- All CSIRTs need funding to exist and operate effectively
- The funding process is:
 1. Create a budget
 2. Create a business plan
 3. Present your budget and plan



Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

1. Create a Budget

- Lay out a multi-year budget, differentiating between operational costs and investment costs
- Don't overcommit and don't pad your budget
- Be as succinct as possible and upfront about all tangibles and intangibles
- Include budget for additional hardware and software
- Include budget for ongoing training



Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

2. Create a Business Plan

- See examples and coaching sites for business plans
- Your Executive Sponsor should be able to assist you
- The business plan should reflect the CSIRTs goals for the organization and how those goals work in conjunction with the budget
- Speak to ROI



Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

3. Present Your Budget and Plan

- Conduct research so that you are able to defend your budget and the necessity of every item
- Present the plan first to your Executive Sponsor to receive feedback from a supportive source
- Then present it to others who have to approve your plans and your funding



Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

Consider CSIRT Workplace and Infrastructure During Planning

Physical location of staff for 24x7 operation: consider the best level of privacy and protection

- People's conversations and notes and files
- Equipment such as laptops, servers, and data-storage devices
- Other equipment:
 - A secured center for operations
 - A separate, secured data center
 - Safe storage of non-electronic data

Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

Consider CSIRT Workplace and Infrastructure During Planning

Physical location of staff for 24x7 operation: consider the best level of privacy and protection

- Staff require appropriate computer systems and software and typical equipment: phone, fax, email
- LAN, firewall, IDS, VPN
- Disk storage and backup and archival system
- File system for non-electronic data
- Additional software

FIRST guidance: <https://www.first.org/membership/site-visit-v2.5.pdf>

Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

Learning Check

What are some examples of a return on investment (ROI) that a CSIRT can provide?



Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

Questions?

What questions do you have about this lesson?



Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

**Section 3:
CSIRT Architecture and Staffing**

Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

Architecture for an Effective CSIRT



1. Operational Framework
- Clearly-defined mission
 - Clearly-defined constituency
 - Organizational home
 - Formal relationships with other teams
2. Services and Policies
- Capabilities and limitations
 - Information-flow process
 - Information-gathering process

Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

Architecture for an Effective CSIRT



3. Quality Assurance
- Frequent measurement and checking of quality
 - Collection of constituency feedback
4. Adaptability and Flexibility
- Future emerging threats
 - Information leading to more effective CSIRT
 - Legal expertise and support
5. Internal Management Support

Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

CSIRT Staff Require Strong Technical Skills

Security

- Basic security principles
- Generic risks and threats
- Encryption methods and implementations
 - Hashing
 - Symmetric and asymmetric encryption

Internet infrastructure

- Network security appliances
- Network applications
- Network infrastructure
- Common network protocols

Intranet infrastructure

- Internal topology



Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

CSIRT Staff Require Excellent Soft Skills

- Essential CSIRT skills:
- Follow procedures and protocols
 - Make common sense and logical decisions
 - Multitask with excellent organizational skills
 - Communicate effectively both orally and written
 - Handle stressful situations with ease
 - Deal with people with diplomacy and patience



Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

Learning Check

How would you balance your CSIRT's resources between reactive services and proactive services?



Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST

Questions?

What questions do you have about this lesson?



Training Module 1, CSIRT Fundamentals, Version 1, © 2016 FIRST