Security Professionals Workshop: Creating a CSIRT

Georgia Killcrece
Temecula, California
April 22-23, 2003
Imagine...

...that the most critical system for your parent organization or constituency has been compromised and sensitive or proprietary data has been accessed.
Purpose

To talk with you about creating a CSIRT
To discuss the stages of development and a framework for building the vision of the CSIRT
To provide insight into some of the key issues and decisions that must be considered
Why Are We Here?

Computer networks are revolutionizing the way business is done, but have also introduced substantial risks.

The use of technology has provided new opportunities for intrusions.

Changes in

- organizational data protection requirements
- local or national laws
- institutional regulations

make it imperative to address security concerns at an enterprise level.
What Can Be Done?

To defend against Internet security threats, organizations can

- keep up to date with the latest operating system patches and product updates
- install perimeter and internal defenses such as routers, firewalls, scanners, and intrusion detection systems
- update and expand computer security policies and procedures
- provide security awareness training to employees, customers, and constituents
- create an organizational CSIRT
What is a CSIRT?

An organization or team that provides services and support, to a defined constituency, for preventing, handling and responding to computer security incidents
Stages of CSIRT Development

- Stage 1: Educating the organization
- Stage 2: Planning effort
- Stage 3: Initial implementation
- Stage 4: Operational phase
- Stage 5: Peer collaboration
What Does It Take to Get Started?
Building Your Vision

- Constituency
- Organizational Model
- Resources
- Funding
- Services
- Management, Constituent Buy-in
- Mission
Base Set of CSIRT Services

Reactive Services
• alerts and warnings
• incident handling
  - incident analysis
  - and at least one of the following: incident response resolution, incident response support, incident response coordination
• vulnerability handling
  - vulnerability response coordination

Proactive Services
• announcements

Security Quality Management Services
• awareness building
• security consulting
Types of CSIRT Roles

- manager or team lead
- assistant managers, supervisors, or group leaders
- hotline, help desk, or triage staff
- incident handlers
- vulnerability handlers
- technical writers
- network or system administrators
- platform specialists
- support staff
CSIRT Models

- Security Team
- Internal Distributed Team
- Internal Centralized Team
- Combined Distributed and Centralized Team
- Coordinating CSIRT
You May Need More Than One Model
About that Incident…Ask Yourself

• How would your organization respond to this type of incident if it happened now?
• Who would respond? Who should respond? Who else needs to be involved?
• What would the response be?
• Who makes these decisions?
• How would you like your organization to respond?
CSIRT Interactions
Questions To Take Away Today

• What do you know about incident handling at your organization?
• What don’t you know about incident handling at your organization?
• What do you need to know?
• Who needs to be involved to get the answers?
• What needs to be changed in the current way your organization provides or does not provide response?
• How would a CSIRT change the response?
• What do you want a CSIRT to do?
Key Issues and Decisions -1

- Who is your constituency?
- What is your mission?
- How will the CSIRT operate?
- What authority does the CSIRT have?
- How will the CSIRT be funded?
- What services will be provided?
- To whom does the CSIRT report?
- What type of activity should be reported to the CSIRT?
- Where will the CSIRT be located?
- Will the team be centralized or distributed?
Key Issues and Decisions -2

- What type of staff will be needed?
- How many staff will be needed?
- How big will the CSIRT staff be?
- Will staff perform other jobs or just CSIRT work?
- What type of equipment should be purchased?
- How should the CSIRT infrastructure be configured?
- What policies and standard operating procedures are needed?
- Who will help design and implement the CSIRT?
- How should the mission and services be communicated?
Dealing with Constraints

Constraints can include

• budgets
• lack of funding
• geographic dispersion of organization
• organizational disagreements or factions
• lack of management understanding and buy-in
• lack of experienced personnel resources
• lack of a clear vision or consensus across the organization
• lack of communication
• established timeframes
There is No Single Recipe for a CSIRT

It depends on your

• needs and requirements
• mission and goals
• available resources and support
What Is Your Vision?
Contact Information

Georgia Killcrece
CERT® CSIRT Development Team
Networked Systems Survivability
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

csirt-info@cert.org
http://www.cert.org/csirts/
+1 412 268-7090