Module 2
Starting with a CSIRT Team

[Presenter Name]
[Date]

Agenda

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

- Outline how to develop policies, procedures, processes, and workflows
- Define methods for building disaster recovery and business continuity plans
- Explain how to create policies for security configurations, including for physical security
- Describe how to build relationships between a CSIRT and its constituency
- Identify ways to work with the wider community, including vendors, law enforcement, press, and academia
- Practice setting up a CSIRT to function optimally

Section 1:
CSIRT Scope and Policy

Establish and Publish Clear Policies and Procedures

- **Policies:**
  - Governing principles
  - May be service-specific
  - Contain attributes and content
  - Require validation
- **Procedures, Processes, and Workflows:** How activities are carried out

Policy Types

Policies that a CSIRT needs to have in place to ensure incident, vulnerability, artifact, and site information is protected:

- Information classification
- Information protection
- Record retention
- Record destruction
- Information dissemination
- Access to information

- Appropriate usage of CSIRT's system
- Computer security events and incident definition
- Incident handling policy
- Cooperation with other teams
- Other miscellaneous policies

Policy Components

Attributes

A policy should outline essential characteristics for a specific topic area to provide all necessary information to help implement the policy.

Content

Content is a definition of behavior in a certain topic area. Content lays out the strategy for a policy.

Validation

When a policy has been defined, it's crucial to test the validity of that policy in a real-world situation.

CSIRT Workplace and Infrastructure Policies

Make sure your security policies match the way your organization works

- Interaction of people and equipment, placement of operations center and data center, and safe storage of non-electronic data
- LAN, firewall, IDS, VPN
- Most secure software and browsers
- Mobile technology, BYOD

CSIRT Workplace and Infrastructure Policies

Make sure your security policies match the way your organization works

- PGP or GPG email encryption
- Backup and archival system and a way to store information in non-electronic form
- Data protection
- Data retention and destruction

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

Clearly Document Your Services

Attribute	Description
Objective	Resolve customer web site outage
Definition	Quickly analyze, identify cause, restore services and document resolution and how to avoid in the future.
Function Descriptions	All the functions listed above are documented in the policies and procedures manual.
Availability	Service is not made available unless QA criteria are verified
QA	On each page submission the current data is stored so only the last page on which "submit" was not pressed will be lost.
Interactions and Info Disclosure	Work with our management and the Organization's PR department to produce press release if the outage was noticeable by customers or if it was detected and documented by a security organization. Our policy is to always reveal the minimal necessary to inform our customers.
Interfaces with other services	As incident is closed data will be entered into our internal data bases, including resolution and how to prevent future outages of this time.
Priority	Customer Web Site outages are priority 1 (on our scale of 1-5)

Policy Example: Disaster Recovery and Business Continuity

For disaster recovery and business continuity, identify risks and build a mitigation and recovery plan in keeping with the needs of your organization

Good example: NASDAQ moved its primary servers further away from its disaster recovery servers

Bad example: NYSE left its disaster recovery plan untested and was down for 2 days during Superstorm Sandy

Establish Disaster Recovery and Business Continuity Policies Up Front

High-level steps to building your disaster recovery and business continuity policy/plan:

1. Define the scope
2. Clearly articulate assumptions
3. Build list of disaster scenarios and recovery goals (SLAs)
4. Define continuity and recovery strategy for each scenario
5. Coordinate plan with other teams
6. Obtain management approval
7. Schedule and execute disaster recovery practice drills
8. Revisit and revise plan at scheduled intervals

Learning Check

When a threat to an organization is detected, how does a policy help? How does a procedure help?

Questions?

What questions do you have about this lesson?

Section 2: Building Relationships

Building the Relationship Between CSIRT and Constituency

Full Authority
- Full permission to act on behalf of constituency
- Typical for in-house CSIRTS

Shared Authority
- Direct support with shared decision making
- Often when CSIRTs are contracted

No Authority
- Acting only in advisory capacity
- Assured strong sponsor within management

An Informed Constituency is Essential

- Outbound communications
  - Email updates
  - Intranet
  - Presentations and workshops
- Inbound data collections
  - Incident feedback
  - Formal periodic surveys
- External communications
  - Media and press releases
  - Security bulletins

Know Your Community Partners

Developing relationships in the community with members of these groups can maximize a CSIRT's effectiveness during incidents

- Vendors
- Law enforcement
- Press
- Academics
- Peers
- CSIRT groups (e.g., FIRST, TF-CSIRT)
- Business-oriented groups (e.g., ISACs)

Learning Check

Questions?

What questions do you have about this lesson?