Module 5
Incident Coordination

[Presenter Name]
[Date]

Agenda

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

- Identify methods for handling major security events
- Describe how to coordinate responses with other CSIRTs
- Define an incident coordination process
- Explain processes for working with vendors
- Clarify how to work with law enforcement
- Identify methods for working with organizations at various levels of influence
- Practice incident coordination steps

Section 1:
Major Security Events

What Is A Major Security Event?

A major security event is any security threat that affects the organization in a way that can cause:

- Significant loss of business
- Financial damage
- Injury to reputation/branding

Types of Major Security Events

Types of major security events include:

- Data breaches
- Website defacement
- Denial of service attacks (DOS, DDOS)
- Target attacks and APTs
- Malware incidents
- Phishing incidents

Types of Major Security Events: Data Breach and Website Defacement

Types of major security events:

- Data breach – sensitive or proprietary data is released to unauthorized people or organizations
- Website defacement – when a web page or set of pages is modified, rendering it unusable or redirecting it to a malicious site

Types of Major Security Events: DoS/DDoS, Target Attacks, and APTs

Types of major security events:

- Denial of service (DoS, DDoS) attacks – when a website is made unavailable by bogus traffic overloading the system
- Target attacks and advanced persistent threats (APTs) – a network attack in which an unauthorized person gains access to a network

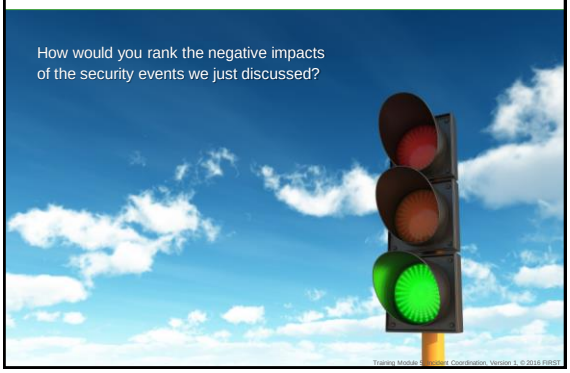
Types of Major Security Events: Malware and Phishing Incidents

Types of major security events:

- Malware incidents – when any software is used to disrupt computer operation, gather sensitive information, or gain access to private computer systems
- Phishing incidents – attempts to acquire sensitive information such as usernames, passwords, and credit card details

Learning Check

How would you rank the negative impacts of the security events we just discussed?



Questions?

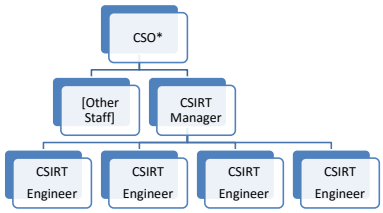
What questions do you have about this lesson?

Section 2: Incident Management and CSIRTs

Coordinating Responses with CSIRTs

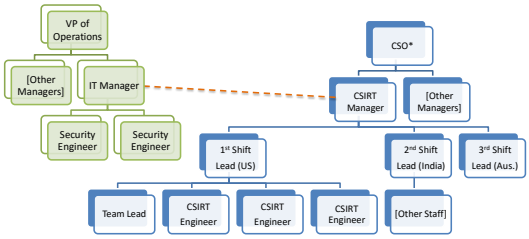
- A CSIRT will vary in size and structure
- Each CSIRT will have a general chain of command where incidents escalate, depending on severity
- PSIRTs may be part of your workflow if your organization releases products
- Make sure you take the time to familiarize yourself with the structure of the CSIRT in your organization

CSIRT Structure: Simple Example



* Organization's Chief Security Officer

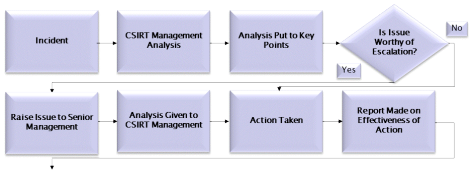
CSIRT Structure: 24x7 Example



* Organization's Chief Security Officer

Flow of Information within CSIRT

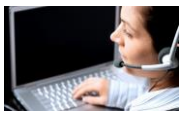
- The way in which information flows within the CSIRT varies from organization to organization



CSIRTs Working in Shifts

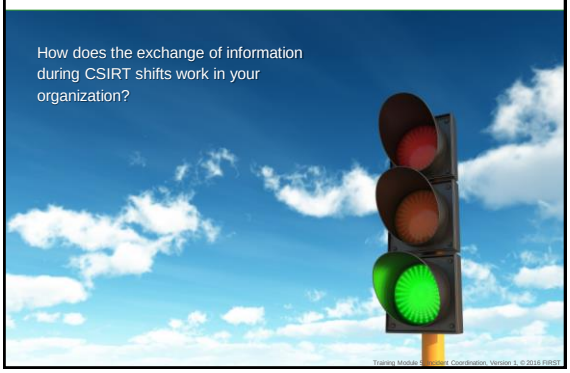
When one member of a CSIRT is working on an incident and a shift change occurs, one of two things must happen:

1. The CSIRT member hands off the incident duties to the corresponding CSIRT member on the next shift
2. The CSIRT stays on in an overtime capacity to finish handling the incident



Note: At no point should any major incident be left without a handler

Learning Check

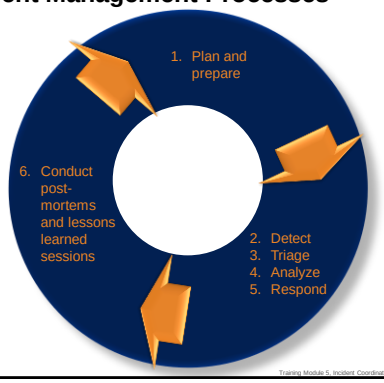


Questions?

What questions do you have about this lesson?

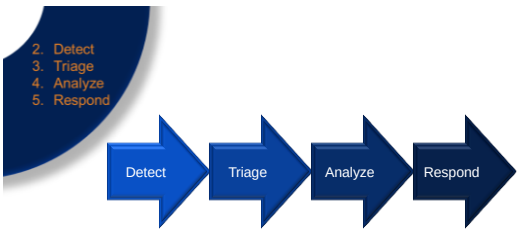
Section 3:
Incident Response Processes

Incident Management Processes

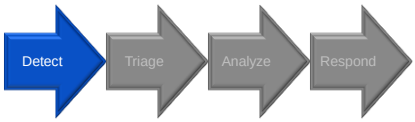


Incident Response Process

There are four phases to every incident response plan:



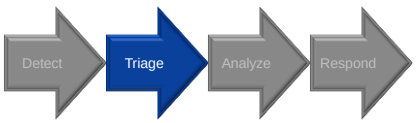
Phase 1 – Detect



The CSIRT must first gather evidence to determine:

- Whether there is an incident
- What type of incident
- Details about the incident

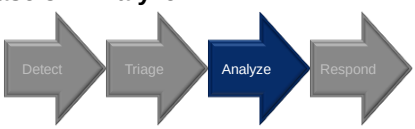
Phase 2 – Triage



The CSIRT must limit the damage to the organization and follow certain steps to make sure the incident is contained:

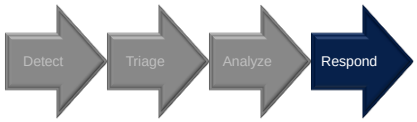
- Short-term containment: limiting the damage as quickly as possible
- Forensic evidence collection: backing up the affected systems and preserving forensic evidence in the event of a criminal act
- Long-term containment: temporarily replacing the systems so normal production can resume

Phase 3 – Analyze



The CSIRT must assess the severity and determine the urgency, identifying the possible causes of the attack

Phase 4 – Respond



The CSIRT must:

- Remove all dangers from the affected systems
- Restore all systems to a permanent operable state
- Bring affected systems back into production carefully
- Test and monitor systems until confidence is restored
- Document the incident and its resolution for future use

Working with Outside Entities

A CSIRT needs to cooperate and coordinate with:

- Vendors
- Law enforcement
- Other agencies or organizations

Working with Vendors

- Vendors are groups that provide products, mainly hardware or software
- If there is a problem with a vendor's hardware or software, go to the vendor's website to look for a fix
- If a fix is not publicized, contact the vendor
- Often the first point of contact is through that vendor's PSIRT

Working with Law Enforcement

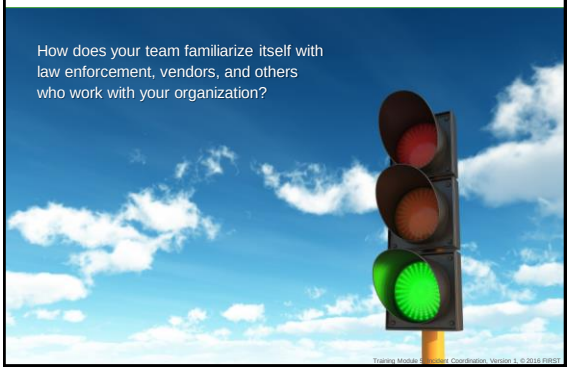
- A CSIRT should contact law enforcement when a crime has been committed
- There are times when law enforcement might reach out to a CSIRT to gather information on a case or offer professional counsel
- The CSIRT might work with state and federal entities, such as the FBI or Interpol
- Organizations have their own processes

Working with Agencies and Organizations

Other agencies and organizations you may work with:

- FIRST
- NERC
- OAS
- ENISA

Learning Check



Questions?

What questions do you have about this lesson?