Incident Command during IT-Related Events

April, 2010
What is Incident Command?

Has your team experienced an event where...

- You needed better communication and organization?
- You needed to provide campus with continual updates?
- People on the team seemed to be working at cross purposes?
- Senior leadership was receiving conflicting status reports from the team?
- No one was sure who was doing what?
What is Incident Command?

Incident Command is a tool that can help...

- Organize efforts and resources
- Assign responsibility for doing, planning, and communicating
- Clarify what is being done and who is making decisions
- Achieve tactical objectives
- Meet the needs of any type or size of incident
- Create a cohesive team quickly
- Provide administrative and logistical support to the operational team
- Avoid duplication of effort
What is Incident Command?

Originated with Homeland Security–Presidential Directive to create a National Incident Management System (NIMS). ICS is a key component that:

- Is a standardized management tool for meeting the demands of small or large emergency or nonemergency situations
- Represents "best practices," and has become the standard for emergency management across the country.
- May be used for planned events, natural disasters, and acts of terrorism.

Note: We use a version of this here at UA–see the CERT website http://cert.arizona.edu
What is Incident Command?

What constitutes an incident?

It is an event or occurrence that...

• Affects a large number of campus constituents
• Requires a coordinated response from more than one department, more than a normal workload to fix, and regular communications to campus until resolved
• Could result in “headline news”
What is Incident Command?

Is it an Incident?

It's a judgment call, but better to say "yes" and have it be short and sweet than to not react appropriately and create more stress!
Incident Command Structure

- Incident Commander
  - Operations Section Chief
  - Planning Section Chief
  - Logistics Section Chief
  - Public Information Officer
  - Scribe
Incident Commander

- Provides overall leadership for the incident
- Takes general direction from senior leadership
- Establishes and maintains IC Post ("war room")
- Establishes regular and necessary IC meetings
- Establishes incident objectives
- Ensures that an Incident Action Plan is developed and followed
- Works closely with the PIO to create campus alerts and timing of messages
- Initiates new Operations Chief(s) and Teams as needed by Incident
- Works closely with Logistics and Finance to acquire resources (personnel or operations) as needed
- Works closely with Planning Chief to determine scope of planning activities
Incident Command Structure

- Incident Commander
  - Operations Section Chief
  - Planning Section Chief
  - Logistics Section Chief
  - Public Information Officer
  - Scribe
Incident Command Structure

Operations Section Chief

- Carries out the incident objectives (For example: Determine the causes of payroll overpayments and determine a corrective action by noon today)
- Organizes, assigns, and supervises tactical team to carry out the objective
- Is typically one of the first organizations to be assigned to the incident
- Expands from the bottom up (For example: we find that there are 3 different kinds of overpayments)
- Has the most incident resources
Incident Command Structure

Operations Section Chief
Incident Command Structure

- Incident Commander
  - Operations Section Chief
  - Planning Section Chief
  - Logistics Section Chief
  - Public Information Officer
  - Scribe
Incident Command Structure

Planning Section Chief

- Manages the planning process
- Compiles the project plan
- Maintains resource status
- Maintains and displays situation status
- Develops alternative strategies and plans as identified by the Incident Commander
- Provides documentation services
- Prepares the Demobilization Plan
Incident Command Structure

Incident Commander

- Operations Section Chief
- Planning Section Chief
- Logistics Section Chief
- Public Information Officer
- Scribe
Incident Command Structure

Logistics Section Chief

- Food for incident personnel
- Supplies
- Facilities
- Provides resources and services required to support incident activities
- Contracts for and purchases goods and services needed at the incident
Incident Command Structure

- Incident Commander
  - Operations Section Chief
  - Planning Section Chief
  - Logistics Section Chief
  - Public Information Officer
  - Scribe
Public Information Officer

- Advises Incident Commander on information dissemination and media relations
- Creates communications and gets them approved by the Incident Commander
- Obtains information from and provides information to community and media
Incident Command Structure

- Attends all incident meetings and takes notes.
- Provides regular incident de briefs as needed by Incident Commander and Public Information Officer.
Recent Incident Commands as Discussion

- **eMail Outage (November)**
  - Broad scale impact
  - Communications
  - Cross-departmental coordination
  - Needed methodical analysis
  - Headline potential
Recent Incident Commands as Discussion

- **www.arizona.edu** (December – March)
  - Broad scale impact
  - Communications
  - Cross-departmental coordination
  - Needed methodical analysis
  - Headline potential
  - Needed outside resources to help
  - Potential for $$$ need was high
Recent Incident Commands as Discussion

- **www.arizona.edu** (December – March)
  - Broad scale impact
  - Communications
  - Cross-departmental coordination
  - Needed methodical analysis
  - Headline potential
  - Needed outside resources to help
  - Potential for $$$ need was high
Recent Incident Commands as Discussion

- **HPC Security Breach**
  - Communications
  - Cross-departmental coordination
  - Possible ITAR issues
  - Needed methodical analysis
  - Headline potential
Recent Incident Commands as Discussion

- Mosaic Performance (April)
  - Broad scale impact
  - Communications
  - Cross-departmental coordination
  - Needed methodical analysis
  - Headline potential
  - Needed outside resources to help
  - Potential for $$$ need was high
How UITS Uses It

• First Responders still act immediately
• Information flows up
• Senior Leadership makes call for creation of Incident Command based on parameters:
  • Scale of Impact (# affected)
  • Potential for headlines
  • Potential for $$$
  • How much communications needs to be done.
  • Need for Cross-departmental coordination
  • Anticipated timeline of event
  • Need for organization in general
• It’s okay to have a 1 day Incident Command (or less)
Things to Think About For This Team

- Will the methodology even help you?
- Who makes the call for IC?
- What is an Incident for Payroll?
- Do you want more training – we have learned as we go with a little help from Brian Seastone.