Incident Command for IT: What We Can Learn from the Fire Department

Brent Chapman
brent@greatcircle.com
Great Circle Associates, Inc.
http://www.greatcircle.com
IT managers often need to manage incidents

Security incidents
Service outages
Infrastructure failures
  Power failures
  Cooling failures
  Connectivity failures
… and so forth
Who manages emergencies daily?

Public safety agencies

Fire departments
- Urban & suburban
- Forest & wildland

Police departments

Coast Guard

… etc.
How do public safety agencies...

Organize themselves on the fly to deal with a major incident?

Quickly and effectively coordinate the efforts of multiple agencies?

Evolve the organization as the incident changes in scope, scale, or focus?

What can IT professionals learn from that?
For example…

A car hits a fire hydrant
  Occupants are trapped and injured
  Water from hydrant floods an underground electrical transformer, causing a short circuit & an outage

Who might be involved in response?
  Fire department – rescue trapped occupants
  Ambulance service – treat & transport victims
  Police department – direct traffic & investigate
  Water department – shut off hydrant
  Electric company – deal with flooded transformer

How to coordinate all that?
What needs to get done?

Ambulance crew needs to treat & transport victims
But first, fire department crew needs to extricate them from wreckage
But before they can do that, water company needs to shut off water
Which they can’t do until electric company safes the flooded transformer
How do you organize this?

Who is in charge?

How do they figure out what needs to be done, and who can do it?

How do assignments get made, so that
  Everything necessary gets done
  No effort gets duplicated
  Everything is done safely
An even bigger example: Southern California Wildfires

Fast-changing situation
- Fire grows and moves as weather and winds shift
- Plan evolves as situation & resources change

Many agencies involved
- Firefighters from dozens of cities, plus CDF, USFS, BLM, and military
- Airborne water drop, transport, & scouting
- Law enforcement to deal with residents
- Support units (medical, kitchens, camps, fuel, etc.)
How about an IT example?

Data center outage — total power failure

Utility service dropped, UPS didn’t take load, generator didn’t start in time
All systems went down hard (no shutdown)

Need to

Ensure services transferred to alternate data center
Cold-start everything; figure out startup order
Check/fix systems as they’re brought back up
Diagnose and permanently fix power problem
Transfer services back from alternate data center

Might take days, involve dozens of people
Other IT examples

Service outages
Security incidents
  DoS attacks
  Virus/worm outbreaks
  Break-ins
Adversarial terminations; layoffs
Not just emergencies
  Facility moves
  Service deployments
  Major upgrades
What do these types of incidents have in common?

Timing might be a surprise
Time matters – need to respond quickly
Situation not perfectly understood at start
  Learn as you go, and adjust on the fly
Resources change over time
  People come and go; not all together at start
Need ways to bring newcomers up to speed
Need ways to transfer responsibilities
So, what is ICS?

Incident Command System
Standardized organizational structure and set of operating principles
Tools for command, control, and coordination of a response to an incident
Provides means to coordinate efforts of multiple parties toward common goals
Uses principles that have been proven to improve efficiency and effectiveness
History of ICS

Developed in 1970’s to coordinate agencies dealing with yearly SoCal wildfires
Has evolved since into national standard
Now used by nearly all US public safety agencies
Often mandated, to obtain state/Federal funding
Key ICS Principles

Modular & scalable organization structure
Manageable span of control
Unity of command
Explicit transfers of responsibility
Clear communications
Consolidated incident action plans
Management by objective
Comprehensive resource management
Designated incident facilities
Key Principle #1: Modular & scalable organization structure

Functions are activated as needed for a particular incident

- All incidents will have a Command Section
- Almost all will have an Operations Section
- Rest of sections are only used on larger/longer incidents

On small incidents, multiple functions often handled by single person
Command Section

Incident Commander (IC) responsible for overall management of incident
IC initially also performs all 4 section chief roles (Operations, Logistics, Planning /Status, Admin/Finance), until each is delegated to somebody else
Operations Section

This is where the real work happens. Operations develops and executes plans to achieve the objectives set by Command. Assists Command in development of Consolidated Incident Action Plan. Typically the biggest section, by number of people. Ops focus is now; Planning worries about later.
Planning/Status Section

Collects & evaluates info needed to prepare action plan
Forecasts probable course of incident
Plans for next day, next week, etc.
Keeps track of what has been done, and what still needs to be done
Keeps “current status & plans” info up to date, so that new arrivals can brief selves
Logistics Section

Responsible for obtaining all resources, services, and support required to deal with the incident. Responsibilities include facilities, transportation, supply, equipment maintenance & fueling, feeding & medical care of incident response personnel, etc.

Is more important on big, long-running incidents; may not be needed on small or short incidents.
Admin/Finance Section

Responsible for tracking incident-related costs (including time & materials, if necessary for reimbursement)

Also administers procurements arranged by Logistics

Usually only activated on the very largest and longest-running incidents
Growing the ICS organization

Initially, the senior-most first responder is the Incident Commander (IC)

IC responsibility may transfer to somebody else later, as incident grows, but that isn’t automatic

Generally better to keep the same IC, if feasible

Stuff gets lost during handoffs

If IC transfer does happen, it needs to be explicit

One person often fills multiple slots on org chart

Initially, IC also heads other sections (Ops, etc.)

Delegates to others as necessary and possible
Key Principle #2: Manageable span of control

Each supervisor should have 3-7 subordinates
5 is ideal
When necessary, as org grows, create new levels
Division might be Functional Geographic
Key Principle #3: Unity of command

On incident, each person has 1 boss
- Strict tree structure, all the way to the top
- Everybody knows who they work for
- Every supervisor knows who works for them

Works better than matrix in an emergency
- Doesn’t assume folks normally work together, or even know each other

Makes communication & coordination easier, up /down tree, as organization grows & changes

Reduces freelancing
Key Principle #4: Explicit transfers of responsibility

Changes to organization are made explicitly

More senior person doesn’t automatically take over upon arrival

Might, but only after briefing on status/plans from person they’re replacing, and explicit turnover (including notifying subordinates and superiors)

Person already in place is often better suited to handle current situation, and certainly is more up to speed

Planning/Status keeps overall org chart updated
Key Principle #5: Clear communications

Communicate clearly and completely, not in code
- Reduces potential for confusion
- Reduces time spent clarifying
- Lets other people (including management) monitor

Talk directly to resources, when possible
- Use the tree to find, then work with them directly
- Using tree also helps keep management informed
Key Principle #6: Consolidated action plans

Command communicates top-level action plan for current operational period (hour, shift, day, etc.)

- Plan states, at a high level, what organization is trying to accomplish right now
- Section chiefs (Ops, Logistics, etc.) help develop plan

Written plan is best

- Makes it easier to keep everybody on target
- Makes it easier for new arrivals to brief selves

Rule of thumb: if it crosses organizational or specialty boundaries, write it down
Key Principle #7: Management by objective

Tell people what you want to accomplish, not how
Let them figure out how to get it done
Gives them room to flexibly and creatively cope with changing circumstances

For example, say “get a public web server back online with an ‘out of service’ notice for our customers”, not “take host xyz123, reload it with RedHat and Apache, move it to rack 7, …”

Is generally faster to communicate, and the folks doing the work may know a better way than you
Key Principle #8: Comprehensive resource management

All assets & personnel need to be tracked
   So new resources can be used most effectively
   So existing resources can be relieved
Folks should “sign in” through Admin function, then wait for assignment
   Helps ensure they’re put to best use
   Might want to designate a “report to” site
   Also simplifies briefing new arrivals
Key Principle #9: Designated incident facilities

Command Post (CP) is key facility to identify – that’s where everybody can expect to find IC

If IC needs to leave CP, needs to transfer IC responsibility (temporarily or permanently) to someone who’ll still be there.

Also useful to designate “staging area” for new resources to report to upon arrival, for sign-in and assignment; may be at CP.
ICS for IT in action…

It’s a Tuesday morning, and everything is normal. The company’s load is split 50/50 between its two data centers, in Sunnyvale and Mesa. At about 9:30am, the NOC loses all monitoring of Sunnyvale, and the load doubles in Mesa. The NOC suspects a network outage, begins to troubleshoot, and pages all NetOps managers, per their SOP. Bryan, the Director of Operations, happens to be nearby, and diverts to the Sunnyvale DC.
9:45am

Bryan arrives at the DC at about the same time as Joe and Tom, two of the company’s installers.

In the parking lot, they notice that the facility’s generator is running.

Inside, they find that the lights are on, but all of the UPS-powered equipment (servers, network, etc.) is without power.
First steps…

Bryan calls the NOC:
1) Informs them he’s activating ICS plan [clear communication]
2) Asks them to page all NetOps personnel to report to DC conference room for assignment [staging area]

Bryan directs Joe and Tom to switch off all systems, then investigate power problems. [serving in multiple roles; management by objective]
10:15am

Cary, the facilities manager, arrives. Bryan asks him to take charge of investigating the UPS failure, while Joe and Tom continue to switch off systems to prevent unplanned restarts.

Paul (the server team manager), Dave, and Karl (server sysadmins) arrive. Bryan asks Paul to direct them in preparing to bring servers back online. [span of control]
10:30am

Chris, the NetOps VP, arrives. After a brief discussion with Bryan, they decide it makes most sense for Bryan to remain as IC, and for Chris to serve as liaison to rest of company. [explicit transfer of responsibility, not automatic upon arrival of more senior personnel]
10:45am

Rich, Colleen, and John from the Networking team, and Bob (the Networking team manager) arrive.

Bryan asks Rich to take charge of Colleen and John as the Networking team on this incident, and asks Bob to handle Planning/Status for the overall incident. [comprehensive resource management, using folks where most needed]
11:00am

Paul needs more help with servers, so Bryan reassigns Tom and Joe to Paul’s team. [comprehensive resource management]

Cary determines that they may need to run on generator power for several days, but that the fuel tank isn’t big enough for that. Bryan calls Jonathan, the group’s purchasing agent, and asks him to take on the Logistics role and arrange for refueling (& lunch!). [modular, expandable organization]
And so forth…

The organization changes, as the situation and resources change
Following the ICS principles gives you a way to keep it all under control
Could keep this going indefinitely, if needed
ICS Tips

Establish ICS early in an incident
   If you get off to a disorganized start, you’ll be playing catch-up forever

Think of ICS as a toolbox full of tools
   Choose the tools you need for the incident at hand
   Keep it simple

Practice ICS at every opportunity
   If you use it for “routine” and pre-planned events like moves, upgrades, and deployments, your team will be more comfortable using it for “surprise” events like outages and security incidents
Learning more about ICS

Free materials and online courses (FEMA):
http://training.fema.gov/EMIWeb/IS/ICSResource

Wikipedia entry describing ICS:
http://en.wikipedia.org/wiki/Incident_Command_System

Amateur Radio (ARRL) perspective on ICS:
http://ema.arrl.org/fd/ICS_TM.htm
These slides are available in my blog:
http://www.greatcircle.com/blog/

Brent Chapman
brent@greatcircle.com
Great Circle Associates, Inc.
http://www.greatcircle.com