The Practical Gamemaster:
Design and Execution of IT Emergency Operations and Drills

presented to BBLISA - Boston Area LOPSA

Adele Shakal
Director, Project & Knowledge Management
Metacloud Inc.

Formerly Technical Project Manager at USC ITS

ITS Great Shakeout 2011

IT Emergency Operations and Drill Designer

Putting Emergency Drills into Context

- **E**mergency **R**esponse
- **E**mergency **O**perations
- **B**usiness **C**ontinuity **P**lanning & **R**esiliency
- **D**isaster **R**ecovery and Information Technology Architecture
- Emergency Planning and Drills
- Zombie Apocalypse

Emergency Response: "Respond"

- Goals
  - First Aid, Shelter and Communication
- Personnel
  - Your organization's Community/Campus/Building/ Amateur Radio Emergency Response Team(s)
    - CERT, BERT, ERT, ARERT or ARECT
  - Security and safety staff
  - Local, state and federal emergency responders and authorities

IT Emergency Operations: "Assess, Report, Recover"

- Goals
  - For People, Places and Things…
  - assess status
  - report status
  - improve the situation according to previously planned priorities
- Personnel
  - All who will participate in emergency operations until your organization returns to "normal operations"

Business Continuity Planning & Resiliency Goals

- Identify Critical Business Functions
  - BIA: Business Impact Analysis
    "where are our priorities?"
- Identify Risks and Likelihoods
  - TRA: Threat and Risk Analysis
    "what's likely to adversely impact them?"
- Identify Recovery Objectives for CBFs
  - RPO: Recovery Point Objectives
    "how much time's worth of data related to this function can we tolerate losing?"
  - RTO: Recovery Time Objectives
    "how long can we tolerate this function being down?"

Business Continuity Planning & Resiliency Personnel

- In-house experts, possibly also outside experts
- Those responsible for implementing organizational solutions
- Those responsible for maintaining policies, procedures and plans

This will likely require strategic and tactical participation from all groups within your organization!

(Also probably cookies.)

Disaster Recovery and Information Technology Infrastructure

- Goals
  - Implement technical designs according to business needs, financial and technical realities
  - Document recovery objectives, processes and designs
  - Include manual and emergency workarounds and processes
- Personnel
  - Information Technology experts
  - Business process managers
  - Emergency planners

Emergency Planning and Drills

- Bring all of these goals and personnel together; be relevant and engaging
- Create a plan, ensure it is current and available
- Hope for the best, plan and drill for the most-likely, and cope with the worst
- Identify leaders

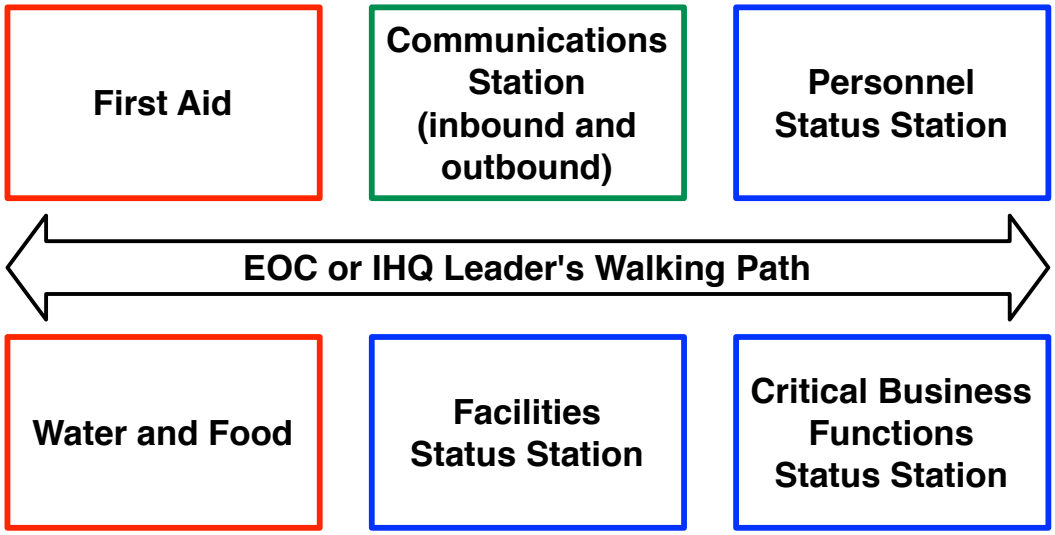
Who will step forward to lead your Emergency Operations Center or Incident Headquarters during a zombie apocalypse?

Designing an Emergency Operations Center or Incident Headquarters

Lessons from other experts:

- Incident Command System (ICS)
- National Incident Management Sysystem (NIMS)
- National Emergency Management Association (NEMA)
- International Association of Emergency Managers (IAEM)
- Citizen Corps
- Community Emergency Response Teams (CERT)
- InfraGard (private sector partnership program with FBI)

Showcase a Simple Emergency Operations Center or Incident Headquarters



- Set it up, provide good food and drink!
- Lead short guided tours for those who will participate in upcoming drills
- Publicize the schedule and participants lists for upcoming life-safety, basic and advanced drills

Designing Stations within the Emergency Operations Center or Incident Headquarters

Capture and Timestamp Prioritized Information & Status:

- Staff
  - By organizational chart, by job function
  - Note their location and connectivity
- Facilities
  - By geographic location, by criticality to restore
  - Note what expertise and resources are needed to restore
- Services
  - By critical business function, by Recovery Time Objective
  - By responsible-organization within organizational chart
  - By staff expertise required to restore

A Gotcha About Designing EOC and IHQ Stations

Stations need to make it easy to capture status updates, but also to make it easy to determine which staff, facilities and services have not yet been heard from.

It is as important to have accurate information from those who've checked in as it is to have accurate information about who has not checked in.

Life-Safety Drill Goals – "Respond"

- Ensure your organization can meet basic Emergency Response needs
  - Facility Evacuations and/or Shelter-in-Place
  - Safe Refuge Locations
  - First Aid
  - Collect and Communicate Personnel Injuries and Locations Status

Basic IT Emergency Ops Drill Goals – "Assess, Report, Recover"

- Activate the Emergency Operations Center or Incident Headquarters
- Collect and Communicate Status:
  - Personnel Availability
  - Facilities
  - Critical Business Functions
- Prepare to communicate with customers and outside entities

"Who is available to help recover this short list of our most critical business functions impacted by this theoretical emergency, and do they have the places they need to work?"

Unknown Terrain: Your Organization May Not Have an Up-to-Date and Accessible…

- List of key personnel's contact information
- Publicized, prioritized list of top critical business functions
- Mapping of which IT services and infrastructure are part of which critical business functions, and who can provide status updates about their recovery

Map Only The Terrain You Need

- Don't try to create a *comprehensive* service catalog for drill purposes if your organization lacks one.
- Do identify organizational leaders to determine top Critical Business Functions, their Recovery Point Objectives and Recovery Time Objectives, and get that documented.
- Do identify the IT infrastructure and/or services, manual workarounds and processes which comprise the top Critical Business Functions, and focus your drill designs around them.
- Don't try to Solve All The Problems.

Designing the Theoretical IT Emergency

- Create “secret notes” for participants to open at set times during the drill, simulating personnel, facilities, and critical business functions updates.
- Chart the “secret notes” ahead of time; during follow-up they will be compared with summary status reports provided by drill participants.
- Allow time at drill start to introduce drill structure, and at drill completion to discuss and capture lessons learned.

An Example Basic “Secret Note” Chart

Time	EOC/IHQ Lead	Facilities	Voice/ Network	Sysadmin/ DBA	Call Center	DevOps/ Apps
10:00am	**Present the Drill Intro**					
10:05am	News update, set up status stations	Building safety and staff update	Staff availability update	(no update)	Staff availability update	(no update)
10:10am	Generate 10:15am status report!	Staff availability update	Services down alerts	Staff availability update	Services down alerts	Staff availability update
10:15am	Generate 10:20am status report!	(no update)	(no update)	Services down alerts	(no update)	Services down alerts
10:20am	**Compare 10:15am and 10:20am status reports to “secret notes” chart & masterlist Discuss lessons learned, suggestions for future drills**					
10:30am	**Conclude Drill**					

Example "Secret Notes"

Time: 10:05am
Team: Facilities

Building 34 has been evacuated; it appears structurally unsound to casual observers and ERT; complete power loss, generators offline; fire alarms are sounding, some sprinklers activated.

Time: 10:05am
Team: Voice/Network & Call Center

Voice/Network call center staff are uninjured and available to work; four technicians in the field have not checked in and are unaccounted for but the rest of that group have checked in with only minor injuries. Staff are in process of checking system status of critical locations' phone service; the main number has failed-over successfully to remote call center.

Time: 10:05am
Team: Sysadmin/DBA

Sysadmin staff in building 32 report no injuries but power loss to the desktop office circuits; two staff members had not arrived to the office and they are staying home, where they have power, landline, mobile phone, internet access.

We've heard no updates from our sysadmin team in building 34.

Time: 10:10am
Team: Facilities, Sysadmin/DBA

Building 34 sysadmin staff report several minor injuries, but all building 34 sysadmin staff are accounted for following building evacuation. All building 34 staff have been instructed to shelter at safe refuge area between parking structure and building 33.

Enact a few basic drills, before tackling more advanced goals.

Designate someone to capture Lessons Learned and Action Items during the drill itself.

Resources will be needed to accomplish follow-up.

Advanced IT Emergency Ops Drill Goals – "Respond and Assess, Report, Recover"

- Include Emergency Response: Facility Evacuations and/or Shelter-in-Place, Safe Refuge Locations, and First Aid
- Activate Emergency Operations Center or Incident Headquarters
- Collect and Communicate Status and Updates:
  - Personnel Injuries and Locations
  - Personnel Availability
  - Facilities
  - Critical Business Functions
- Prepare to interface with customers, vendors, partners and other outside entities

Advanced drills can be intense. Schedule them appropriately; how often is necessary, how infrequently is acceptable?

Designate someone to capture
Lessons Learned
and Action Items
during the drill itself.

Resources will be needed to accomplish follow-up.

If Appropriate to your Organization, Enact Guru-Level ~~Games~~ Drills

- Prepare to interface with media, local, state and federal authorities, and charitable emergency and disaster response groups.
- Consider introducing conflicting status updates.
- Consider introducing slightly-variable delays of incoming status updates to your Emergency Operations Center or Incident Headquarters.
- Consider simulating lack of personnel and/or facilities availability… you may need to randomize this.

(You do have plenty of dice, don't you?)

An Example Advanced “Secret Note” Chart

Time	EOC/IHQ Lead	Facilities	Voice/ Network	Sysadmin/ DBA	Call Center	DevOps/ Apps
11am	**Present the Drill Intro**					
11:10+	News update, set up status stations	Building safety and staff update	Staff availability update	Staff availability update	Staff availability update	Staff availability update
11:20+	Generate 11:30 status report!	Staff availability update	Services down alerts, staff update	Services down alerts, staff update	Services down alerts	Staff availability update
11:30+	Generate : 11:40 status report!	Staff availability update	Restores in progress update	Restores in progress update	Restores in progress update	Services down alerts
11:40+	Generate 11:50 status report!	Building safety update	Restores in progress update	Restores in progress update	Restores in progress update	Restores in progress update
11:50+	**Compare 11:30, 11:40, and 11:50 status reports to “secret notes” chart & masterlist Discuss lessons learned, suggestions for future drills**					
noon	**Conclude Drill**					

So, About that Zombie Apocalypse…

- Keeping a large group of very intelligent IT folks engaged in a drill simulation can be challenging!
- Design **likely** emergency scenarios.
  - Be mindful and respectful of your participants' time.
- Design **realistic** function failure scenarios.
  - If a critical business function status is "up" but its prerequisite IT infrastructure is "down", your technical drill participants will disengage!
- But… keep things a little lively and creative.

(If necessary, throw in some falling satellites, alien invasion and zombie apocalypse jokes.)

Questions?

Slides available at adeleshakal.com

adele@alumni.caltech.edu
adele.shakal@gmail.com