LISA '13
27th Large Installation System Administration Conference
November 3–8, 2013 • Washington, D.C.

Becoming a Gamemaster:
Designing IT Emergency Operations and Drills

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

usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Putting Emergency Drills into Context

- **E**mergency **R**esponse
- **E**mergency **O**perations
- **B**usiness **C**ontinuity **P**lanning and **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 **C**ommunity/**C**ampus/**B**uilding/ **A**mateur **R**adio **E**mergency **R**esponse **T**eam(s)
  - 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
  - **B**usiness **I**mpact **A**nalysis – "where are our priorities?"
- Identify Risks and Likelihoods
  - **T**hreat & **R**isk **A**nalysis – "what's likely to adversely impact them?"
- Identify Recovery Objectives for CBFs
  - **R**ecovery **P**oint **O**bjectives – "how much time's worth of data related to this function can we tolerate losing?"
  - **R**ecovery **T**ime **O**bjectives – "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

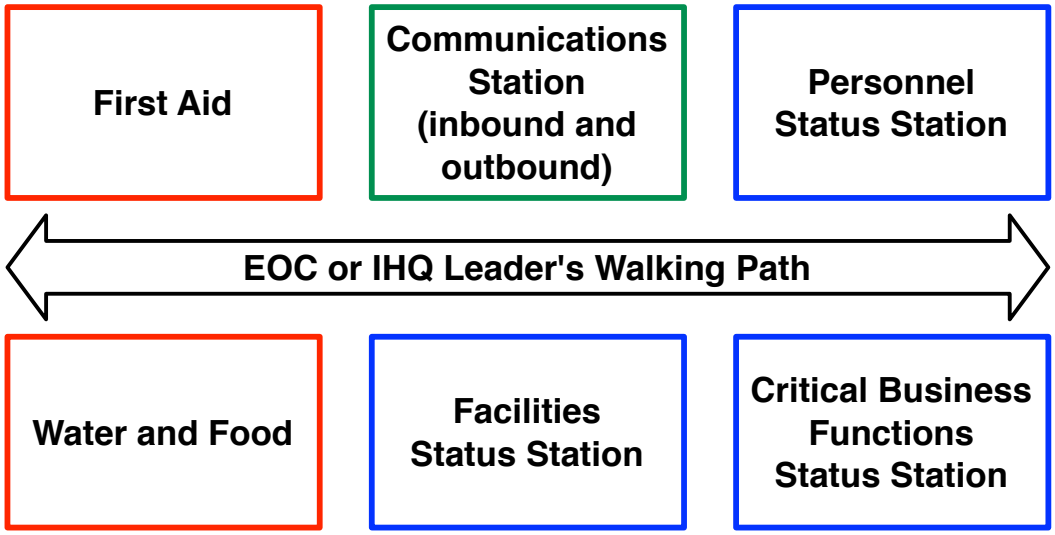
- Bring all of these goals and personnel together; be relevant and engaging
- Create a plan, ensure it is current and available
- Hope for the best, plan and drill for the most-likely, and cope with the worst
- Identify leaders who will head up your **E**mergency **O**perations **C**enter or **I**ncident **H**ead**q**uarters in event of Zombie Apocalypse

Designing an EOC or IHQ

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)

Showcase the EOC or IHQ



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

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 EOC or IHQ
- Collect and Communicate Status: Personnel Availability, Facilities, Critical Business Functions
- Assign Resources to Recover Prioritized Services Required by Critical Business Functions
- Prepare to communicate with customers and outside entities

"Who is available to help recover this short list of 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 new, comprehensive service catalog for drill purposes if your organization lacks one.
- **Do** identify organizational leaders to determine the top Critical Business Functions, their Recovery Point Objectives and Recovery Time Objectives; get that documented.
- **Do** identify the IT infrastructure and/or services, manual workarounds and processes which comprise those 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 "Secret Note" Chart

Time	EOC/IHQ Leader	Facilities Team	Voice & Network Team	Sysadmins & DevOps Team	DBA Team	Apps Team
3:00pm	**Present the Drill Intro**					
3:10pm	News update, set up status stations	Building safety and staff update	Staff availability update	(no update)	Staff availability update	(no update)
3:20pm	Generate 3:30pm status report!	Staff availability update	Services down alerts	Staff availability update	Services down alerts	Staff availability update
3:30pm	Generate 3:40pm status report!	(no update)	(no update)	Services down alerts	(no update)	Services down alerts
3:40pm	Compare 3:30 and 3:40 status reports to "secret notes" chart & masterlist Discuss lessons learned, suggestions for future drills					
4:00pm	**Conclude Drill**					

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 EOC or IHQ
- Collect and Communicate Status: 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?

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

- Interfaces with media, local, state and federal authorities, and charitable emergency and disaster response groups
- Conflicting status updates
- Slightly-variable delays of incoming status updates to your EOC or IHQ
- Simulations of lack of personnel and/or facilities availability… you may need to randomize this

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

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**.

Questions?

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