Emergency Management 101

Everything You Need To Know For A Solid Program
Agenda

• Hazard analysis – match the planning to the risk
• Bringing together the silos
  – Emergency Response
  – Business Continuity
  – Disaster Response
  – Crisis Communications
• Incident Management and the Incident Command System
• Training and Exercises
Before you do anything - assess!

• Before you plan your response you must assess your risks:
  – Natural hazards
  – Your neighbors
  – Human risks
  – Environmental risks
  – Political/country risks
  – Your building

• Determine likelihood of risk & plan accordingly
Natural Risks

- Earthquake
- Volcano
- Tidal Wave - Tsunami
- Wildfires
Natural Risks

- Weather
  - Hurricane
  - Tornado
  - Flood
  - Snow/ice storms/winter storms
  - Lighting
  - Mudslides
  - Wind damage
  - Solar storms
Neighbor Risk

- Who are your neighbors in a one mile radius?
  - Train tracks
  - Freeways
  - Manufacturing
  - Consulates/ Embassy’s/
    Government Buildings
  - Controversial companies
Neighbor Risk

• How about a bit farther?
  – Military bases (10 miles)
  – Airports (10 miles)
  – Nuclear power plant (50 miles)
Human Risk

- Terrorism: **B-NICE**
  - Biological
  - Nuclear
  - Incendiary
  - Chemical
  - Explosive
- Anthrax
Human Risk

• Bomb threats
  – Do you have a bomb threat assessment plan in place?
  – Threat Assessment Team?
  – www.atf.gov
Human Risk

• Violence at work
  – Murder #1 cause of death at work for women
  – #2 cause of death for men

• FBI data for all assaults at work 1,744,300 (900 were murders) FBI1999
Human Risk

• Robbery
  – Thefts

• Labor dispute
  – Strikes

• Sabotage
  – Cyber
  – Product

• Kidnapping
  – Extortion

• Embezzlement
  – Fraud

• Power Outage
  – Human failures
Environmental Risks

- Asbestos
- Polychlorinated Biphenyls (PCB’s)
- Indoor Air Quality (IAQ)
  - Toxic mold
  - Sick building syndrome
Environmental Risks

- Community health risks
  - SARS
  - TB
  - Influenza A, pandemic
Geo/Political

- Political environment
- Social environment
- Economic environment
- Human rights
- Brand protection/trademark issues
- Counterfeiting
Building Security

- Security officers
- Security alarms/cameras
- ID Badges
  - Card access
  - Visitor badges/escorted?  
  - Enforced?
- Perimeter security
- Vulnerable areas of building secured?
  - Loading docks
  - Air intakes
Data Security

- Data center physical security
- Information security breach
- Network security
  - Hacking
  - All of the potential computer critters (worms, viruses, etc.)
- Password policies
- Change procedures
- Data transit protection
- Appropriate back-up procedures
Client/Customer Exposures

• Who are your clients?
• Who do they have as clients?
• Groups who are known to target companies
  – SHAC
  – PETA
Building Life Safety

• Now take time to look at your building carefully. What are the life safety systems?
  – Fire sprinklers
    • Other fire suppression systems
    • Emergency water/cisterns
  – Fire panels/alarms
  – Public address systems
  – Generators/UPS
    • Diesel fuel
  – Chemicals on-site?
Building Life Safety

• Specific to your risks
  – Seismic bracing
  – Hurricane roof support
  – Tornado roof support
  – Row boats for flooding (just kidding)
Out of Danger Comes Opportunity

You're probably thinking to yourself… the only thing she hasn't mentioned is a locust invasion!
Risk Mitigation
Risk Mitigation

• Mitigate risks *when possible* to do so.
• The equation you should keep in mind is...
  – You need to determine
  – risk versus
  – life safety versus
  – cost versus
  – convenience
Business Impact Analysis
Definition

• A Business Impact Analysis is a process designed to:
  – Identify critical business functions and workflow,
  – Determine the qualitative and quantitative impacts of a disruption
  – Prioritize and establish recovery time objectives.
Tell Me More…

• What is a BIA?
  – Each function in a department is examined to determine its time sensitivity and therefore how soon it must be recovered after an event.
  – As it is impossible to restore the entire business at once, the most time critical functions are restored first after a business interruption
A BIA examines…

- Implications of an outage
  - Cost
  - Legal
  - Reputation

- Ranks the recovery as:
  - Survival mode (up to 7 days)
  - Transition mode (one to two weeks)
  - Business as usual (30 days plus)
BIA

- Short description of the department
- List all of the function(s) the department performs
- List the Give/Get relationships between each department and other departments within the company
- Are there any functions within your department that have legal ramifications for the company?
BIA

• Are there any functions within the department that have reputational ramifications for the company?

• What are the financial implications to the company if the functions is not performed?
BIA

• If applicable what is the average daily dollar volume processed by your department?
• If applicable what is the average daily item/transaction volume processed by the department?
• Are there peak times (day, week, month) and/or peak volumes (transactions that exceed a certain level)?
BIA

• Are you aware of any points of risk/failure that may exist within the department? (Example: single points of failure such as only one critical vendor or one employee.)

• If you were unable to occupy the office for a period of time, what options would you consider for the department?
Validate BIA

- Review findings with executives
  - Confirm mission critical business functions
  - Validate time frame
- Essential to validate with executives due to the costs involved in recovery
  - General rule - the quicker you need to resume business the more costly
The Silos of Emergency Management
Out of Danger Comes Opportunity

See a problem?
• What is included in your emergency response program?
  – Basic emergency procedures for all staff
  – Employee training and/or materials
  – Basic first aid supplies
  – Floor warden/emergency response teams (ERT)
  – Written procedures for ERT
  – Training for ERT based on their role
• What is included in your emergency response program?
  – Drills - fire, earthquake, tornado, radio
  – More specialized disaster type supplies
  – Company emergency responder team
  – Specific emergency procedures for all company responders including building specific information
  – Emergency exercise to test teams and procedures
Emergency Pyramid

Who receives their information; how; when; where?

Company Responders

Floor Wardens/ERT

Employees

Out of Danger Comes Opportunity
• The complexity of your DR plan has a lot to do with your size.
• It goes without saying that the bare minimum DR plan is nightly back up with tapes stored off site.
  – Small firms may simply do back up nightly and a staff person takes the tapes off site.
  – Moderate size may have a document storage company take them off site to a warehouse.
  – Large firm may have a contract with a “hot-site” restoration vendor.
• What is included in your disaster recovery program?
  – Authority to Declare a Disaster
  – Clearly identified priorities for recovery of applications and data
  – Recovery Tasks & Procedures: infrastructure and data restoration and resynchronization of data
Out of Danger Comes Opportunity

– Complete inventory list of your equipment and applications.
– A schematic map of the server farm (in case you have to configure one from scratch!)
– Temperature monitoring of the server farm with an alarm notification system, check out www.temperatureguard.com
– Pre-designated “hot site” to recover your data or a drop ship arrangement for equipment
– Regular testing of equipment, procedures and staff
– Up-to-date documentation on recovery of systems and applications including procedures and equipment

Telecommunications recovery strategies for all mission critical numbers
Disaster Recovery Pyramid

Who receives the information; how; when; where?

Telecommunications

Data

Systems
• What is included in your business continuity program (BCP)?
  – Clearly identified mission critical functions that are “time-sensitive”
  – Individuals assigned to a BCP role in each mission critical department
  – Detailed work area recovery plans
• What is included in your business continuity program (BCP)?
  – Individual plans that support the timely recovery of those identified time-sensitive mission critical functions. Plans identify:
    • Staff
    • Equipment
    • Technology and data required
    • Work area recovery strategy
    • Employee communication
    • Vendor communication
    • Critical operating procedures for time sensitive functions
    • Regular exercises of the plan
Out of Danger Comes Opportunity

Business Continuity Pyramid

Who receives the information; how; when; where?

Department Managers

Department Plans

People
What is “crisis-communications?”
  - Communication strategies that reduce the likelihood of an internal business problem going "public" or minimize the reaction if disclosure of the “crisis” cannot be avoided.

The Plan should include:
  - The crisis communication team
  - Positioning
  - Designated spokespersons
  - Media policies and procedures
  - Identified key audiences
  - Draft communications including media, employee, investors and other key stakeholders
  - Collateral materials
  - Contact log
  - Guidelines for speakers presentations and handling media interviews.
Communication Ideas

• Employee hotline 800#
• Employee call trees
• Notification systems
• Web site
• Advance planning to call forward phones (to where?)
• Conference call bridges
• Web-casting

• Sat phones
• Text messaging
• Instant messaging
• Voice over Internet (VOIP)
• Blackberries/Treo
• Nextel phones or those carriers with direct connect feature
Crisis Communications Pyramid

Who receives the information; how; when; where?

Media & stakeholders
Management
Employees
Do you see a coordination problem?

• More than likely yes…
• This lack of coordination is common problem in our industry with all of these silos and no organized centralized management.
What is the solution?

• A incident management program that brings all of the silos together.
What is Incident Management?

• Organized and centralized approach that allows for:
  – Control
  – Coordination
  – Communication
  – Collaboration

• Clear definitions of roles and responsibilities and identified process is essential
Terminology

- Move away from crisis!
- Tiered approach - Incident Response Teams
  - Local incident response team (LIRT)
  - Corporate incident response team (CIRT)
  - Executive Management Team (EMT)
How will this all be organized?
Incident Command System

• To demonstrate that the Incident Command System (ICS) provides an ideal structure in a business setting for:
  – Command
  – Control
  – Coordination/Collaboration
  – Communication
National Response Plan (NRP)

  – creation of a National Response Plan (NRP)
  – integrate Federal Government domestic prevention, preparedness, response, and recovery plans
  – one all-discipline, all-hazards plan

• The purpose of the NRP
  – enhance the ability of the United States
  – prepare for
  – manage domestic incidents
  – establishing a single, comprehensive national approach.

• Plan completed January 6, 2005
  www.nemaweb.org/docs/national_response_plan.pdf
National Incident Management System (NIMS)

- *National Incident Management System (NIMS)* will be developed to provide
  - *consistent* nationwide framework to
  - *standardize* incident management practices and procedures
  - ensure that Federal, State, and local governments can work *effectively* and *efficiently* together
  - *prepare* for, *respond* to, and *recover* from domestic incidents, regardless of cause, size, or complexity
- NIMS adopted the basic tenets of the *Incident Command System (ICS)* as its foundation.

Reflect on those Concepts…

Single Plan

“All Hazards”

Effective

Consistent

Standardized

Integrated

Efficient

Comprehensive

Prepare

Respond

Recover

June 2006
Incident Command System History

• The Incident command System (ICS) was developed in response to a series of fires in Southern California in the early 1970s by an interagency effort called FIRESCOPE.
ICS History

• ICS was designed to manage rapidly moving wildfires and to address reoccurring problems.
  – Too many people reporting to one supervisor
  – Different emergency response organizational structure
  – Lack of reliable incident information
  – Inadequate and incompatible communications
ICS History

- Lack of structure for coordinated planning among agencies (departments)
- Unclear lines of authority
- Terminology differences among agencies (departments)
- Unclear or unspecified incident objectives.
Sound familiar?
ICS Essential Requirements

The designers had four essential requirements:

1. The system must be organizationally flexible to meet the needs of incidents of any kind and size.
2. Agencies must be able to use the system on a day-to-day basis as well as for major emergencies.
3. The system must be sufficiently standardized to allow personnel from a variety of agencies and diverse geographic locations to rapidly meld into a common management structure.
4. The system must be cost effective.
ICS Today

- ICS is now widely used throughout the United States by fire agencies, law enforcement, other public safety groups and for emergency and event management.
- The Department of Homeland Security (DHS) Presidential Directive #5 requirements are a major driving force.

ICS is Required!

• Federal law mandates the use of ICS for all hazardous material incidents (1910.120(q)(3)).
• The State of California requires it in all city and counties.
• Compliance with NRP and HSPD-5 will be:
  – mandatory for all federal agencies and in order to remain eligible for federal funding,
  – state governments must modify existing incident management and emergency operations plans within a year of NRP implementation (January 2006).
What is ICS?

• ICS is a well organized, team approach for managing critical incidents. It has the following hallmarks:
  1. Manageable Span of Control
  2. Common Terminology
  3. Modular/Scalable Organization
  4. Integrated Communications
  5. Unified Command Structure
  6. Consolidated Action Plans
  7. Pre-designated Command Centers
  8. Comprehensive Resource Management
Manageable Span of Control

• A manageable span of control is defined as the number of individuals one supervisor can manage effectively.

• The number of subordinates one supervisor can manage effectively is usually 3-7, the optimum is 5.
Common Terminology

- *Common terminology* is essential in any system, especially when diverse groups are involved in the response.
  - Multiple company departments and/or locations
- Also critical when it is not an activity you perform on a “regular” basis.
- When possible, minimize use of abbreviations, acronyms or confusing terminology to improve communication.
Modular/ Scalable Organization

- A modular organization develops from the top-down at any incident.
  - All incidents regardless of size or complexity will have an incident commander
- The organization can expand/shrink according to the needs of the situation.
- Only activate what you need.
Integrated Communications

• *Integrated communications* is a system that uses standard operating procedures, a common communications plan, common equipment and common terminology.

• Several communication technologies may be established, depending on the size and complexity of the organization and the incident.
Unified Command Structure

• *A unified command* allows all departments or groups with responsibility for the incident, to manage an incident by establishing a common set of incident objectives and strategies.

• Unified command does *not* mean losing or giving up agency (departmental) authority, responsibility, or accountability, it simply provides for a coordinated response.
Consolidated Action Plans (AP)

• *Consolidated AP’s* describe response goals, operational objectives, and support activities.
  – Include the measurable goals and objectives to be achieved. They are always prepared around a timeframe called an *operational period*.
  – Operational periods can be of various lengths, but should be no longer than 24 hours. Twelve-hour operational periods are common for large-scale incidents. At the beginning of an incident the time frame is often short, 2 - 4 hours.

• The Incident Commander determines the length of the operational period based on the complexity and size of the incident.
Pre-designated Command Centers

• *Pre-designated command centers* that are appropriate for the risk and hazards.
  – Ideally have two; a primary and a backup.
  – Determine location once you have done a hazard analysis.
Comprehensive Resource Management

• *Comprehensive resource management* allows an organization to:
  – Maximize resource use.
  – Consolidate control of single resources.
  – Reduce the communications load.
  – Provide accountability.
  – Ensure personnel safety.
ICS allows for…

1. Manageable Span of Control
2. Common Terminology
3. Modular/Scalable Organization
4. Integrated Communications
5. Unified Command Structure
6. Consolidated Action Plans
7. Pre-designated Command Centers
8. Comprehensive Resource Management
Incident Command System
Five Functions of ICS

- Command
- Operations
- Planning & Intelligence
- Logistics
- Finance
The One Word Definition

- Command
  - Manages
- Operations
  - Does
- Logistics
  - Gets
- Planning & Intelligence
  - Plans
- Finance
  - Pays
ICS Organizational Chart
Command

- Sets priorities and objectives and is responsible for overall command and responsibility of the incident.
- In charge of all functions.
- Directs, controls, orders resources.
- Resolves conflict.
- Implements policy decisions.
- Provides interface to Executive Management.
Operations

• Has responsibility for all *tactical* operations necessary to carry out the plan (response and recovery).
  – Involves the key “backbone” aspects of the business - facilities, security, IT, telecom.
  – Initial damage inspection.
  – Establish situation control.
  – Develop situation status reports (sit reps)
  – Front line- resolve the issues.

• Goal - restore business back to “business as usual”
Planning & Intelligence

• Responsible for the collection, evaluation, and dissemination of information concerning incident development.
  – Develop & maintain intelligence plans (BCP, DR plans).
  – Takes situation reports and evaluates information.
  – Applies “intelligence” to the situation and action plans.
  – Make recommendations for action based on event & plans.
Logistics

• Responsible for providing the necessary support (facilities, services, and materials) to meet incident needs.
  – Get whatever it takes to recovery from the event.

• Primary responsibility is the “care & feeding” of the teams.
  – All of the human aspects of the disaster.
Finance

- Responsible for monitoring and documenting all costs. Provides the necessary financial support related to the incident.
- Establishes a paper trail for all expenditures.
- Payroll, emergency purchase orders and cash, “P” cards and other critical cash issues.
- Works with insurance companies regarding reimbursement & worker’s compensation insurance.
Yikes...what is all this?
ICS Benefits

• Flow of information & resources within & between all groups & at all levels both horizontal & vertical.
  – Especially helpful for companies with multiple locations.

• Coordination between groups and all levels.

• Rapid mobilization, deployment & tracking of resources.

• Development of trends & patterns.

• Minimizes confusion & errors.
How does this solve the silo issue?
Corporate ICS Models
Large International Insurance Company

Command
- Legal
- Sr Comm

Executive Mgmt.

Operations
- Real Estate
- Facilities
- IS
- Telecom
- Corp. Security
- Safety & Health

Logistics
- HR
- Employee Relations
- Corp Meeting & Travel
- Aviation
- Admin Supp.

Planning/Intelligence
- BCP
- Corp Comm.
- Insurance
- Legal
- Security
- Six Strategic SBU’s

Finance
- Finance
- Purchasing/Procurement
- Payroll

June 2006
Large Multinational Bank

Senior Mgmt

Command

Operations
- Facilities
- Security
- Telecom
- IT

Intelligence-Planning
- Business Priorities
- Legal
- Corporate Relations

Logistics
- Human Resources
- Travel
- Message Center

Finance
- Finance / Procurement
- Insurance

Out of Danger Comes Opportunity
Out of Danger Comes Opportunity

National Mortgage Company

Command

Executive Mgmt

Planning & Intel
- Team Leader:
  - Mortgage Bank:
  - Investment Portfolio:
  - Capital Markets
  - Consumer Group:
  - Shared Services:
  - Credit Risk:

Operations
- Team Leader:
  - Facilities:
  - Physical Security/Safety:
  - Operations:

Logistics
- Team Leader:
  - Logistics:
  - HR:
  - Message Center /Admin Support:

Finance
- Team Leader:
  - Purchasing:
  - Risk Management:
  - Payroll:
  - Accounting:
  - A/P:

IT
- Team Leader:
  - Operations:
  - Applications:
  - Information Security:
  - Purchasing:

June 2006

www.ems-solutionsinc.com
Incident Response Teams

• Who should be in the Incident Response Team (corporate)?
  – Think of the departments who need to be present

• Where should senior management be?
  – Think bubble to the side! Give them clear direction and guidance.
Where are the Executives?

• Executive Management Team is *usually* not part of your incident response team. They have three overall responsibilities:
  1. Strategic and policy oversight (and large expenditure requests)
  2. Media spokesperson
  3. Senior statesperson role to all key stakeholders- employees, major customers, investor community, board of directors, etc
Initial Assessment Team & Severity Levels
Initial Assessment Team

- Who is on the team?
  - Think back bone assessment (facilities, security, IT, Telecom) and then others depending on risks
- IAT assignment
  - Conduct initial assessment
  - Criteria for plan activation
  - Escalation strategies
- How do they work together?
  - How are they connected?
  - Conference bridge - virtual team at first?
- Any of the members can activate the plan and the EOC.
Example of Emergency Levels

• **Level 1:** An emergency that is *limited in scope* and can be addressed by the normal response of the organization. Examples would include a minor fire or a temporary power outage.

• **Level 2:** An emergency that is *moderate to severe* in scope. Examples would include a moderate fire that closes parts of a building, a moderate earthquake with some damage.

• **Level 3:** A *catastrophic disaster* that has severely damaged a mission critical facility requiring relocation of staff and business processes and/or severe disruption of services at that facility.
Training and Exercises
Training and Exercises

• Train all employees on the plan
• There is only two ways to know if any of this works
  1. Have a disaster
  2. Do at least one exercise per year
• We recommend #2, less stressful, more productive!
• Practice! Bi-annual…
  – Telephone tree tests
  – Tape recovery tests
  – Tabletop exercise reviews with staff
Lastly…It’s An On-going Effort

• Develop a maintenance schedule; someone needs to be responsible for a bi-annual review.
• Remember…the work is never done!
Thank You!

Regina Phelps CEM RN BSN MPA
Emergency Management & Safety Solutions
San Francisco, California
415-643-4300 www.ems-solutionsinc.com