POA – CRISIS MANAGEMENT

CHAPTER 1 EMERGENCY MANAGEMENT – THEORY AND PLANNING

United States – beginning of 19th c. when Congress allocated funds for a disaster.
Cold War – civil defense shelters.
FEMA – Federal Emergency Management Agency – 1979.

Importance of Emergency Management

- Emergency procedures – planned and tested.
- EOPs – Emergency Operations Plans.
- Protect the profitability of the enterprise.
- Improvise and remain flexible.
- **The need to resume normal operations rapidly is as great as the need to control potential damage.**
- Decisions that minimize loss.
- Define "emergency"
- Establish an organization to perform specific tasks.
- Establish a method for using available resources and obtaining additional.
- Means for moving normal operations into and back out of the emergency mode of operations.

Elements of Emergency Management
Can be applied to Business Continuity as well.

- Mitigation – avoiding or lessening the impact. Seeks to fix the cycle of disaster damage, reconstruction, and repeated damage.
- Preparedness – plan, organize, equip, train and exercise.
- Response – short-term, direct efforts, immediate actions, execution of EOP.
- Recovery – near-term and long-term actions taken to return the organization to a pre-emergency level of operation.

Business Continuity – private sector version of emergency management.
Business Impact Analysis (BIA)
Continuity of Operations (COOP) – used by federal government.

Objectives of Emergency Management

- minimize the probability of a threat or emergency.
- (Conduct a Risk analysis).
- Mitigate the impact if the event occurs.
- Recover from emergency and resume normal operations.

Types of Threats and Contingencies

1. Natural.
2. Human (internal or external)
3. Accidental.

Emergency Operations Plans (EOP)

- not intended to cover situations addressed in the normal course of business.
- Not every organization needs all types of plans.
- Separate from the organization's Security Operations Plan.
- All-Hazards Approach – adopted by FEMA.
    - Basic emergency plan.
    - with functional annexes (ie. Emergency call lists).
    - And threat-specific annexes (ie. Bomb incidents).
- Stand Alone Plans – for each emergency or contingency.
- OR: a combination of both.
- Simplest way possible.
- Dissemination and distribution.
- Maintain, review and update regularly.
- Formal audit = at least ANNUALLY.
- Management team must participate in plan preparation. (requirements of the organization).
- Continuing process that is never finished as long as the plan exists.
- Periodic drills and exercises, unannounced tests.
- Rehearse as close to actual as safely possible.
- External agencies should not be contacted unless they are told it's a drill.
- Priorities:
    - Protect human life.
    - Prevent or minimize injury.
    - Reduce exposure of assets.
    - Optimize loss control.
    - Restore normal operations as quickly as possible.
- Emergency response systems = people, equipment, and procedures.
- Planning assumptions reduce the "what-ifs".

Emergency Management Structure

- one person designated as the organization's **emergency coordinator**.
- ie. Head of security or engineering.
- Top management must give complete support.
- Committee of representatives from critical departments (a totally new organization should not be developed to handle emergencies).
- Designate alternates.
- Train and test.

Incident Command/Management

Incident Command System (ICS) – expandable structure used as needed.

- Command.
- Operations.
- Planning.
- Logistics.
- Finance and Administration.

- Several staff position that report directly to Incident Commander:
    - public affairs, safety, and liaison.
- In public safety, the IC is usually the highest ranking member of the responding agency.
- **Single-Incident Command** – one agency.
- **Unified Command** – multiple agencies or jurisdictions.
- all organizations should have an internal incident management system.
- Crisis Management Team (CMT) – provides support to the Incident Commander who manages the organization's response. (ie. Senior management, HR, public affairs, legal, etc).
- NIMS – National Incident Management System (DHS, March 2004) – provides a systematic, proactive approaach guiding departments and agencies at all levels of government, the private sector, and nongovernmental organizations to work seamlessly….
- National Response Framework – details a unified national response.

Emergency Operations Centers and Command Posts
EOC – Emergency Operations Center.
CMC – Crisis Management Center.

- designate one or more alternate locations.
- Backup power and potable water, lodging and feeding, if nec.
- Communications is one of the most important ingredients in effectively managing an emergency event.
    - Interoperability – ability for different agencies to communicate.
    - SAFECOM – DHS public safety interoperability initiative.
    - Have FX Foreign Exchange lines available.
- Emergency succession lists.
- Telephone numbers for key personnel.

Liaison and Coordination
Information should be obtained from various agencies.

- representatives from each agency should visit the facility and be aware of the layout.
- Mutual Aid – assist each other. Government agencies often use interagency support agreements or memoranda of understanding.

Public Affairs/Media Relations

- single source in the organization for the orderly release of information.
- Avoid using the term "no comment".
- Media logistics and an area for media briefings.

Family and Victim Support
FEMA, Red Cross, designated organizational point of contact.

Emergency Medical Services

- ascertain the type of in-house medical services.
- Medical supplies and training.
- Consult legal re: liability, licensing, and certification.
- Contact local hospitals – ascertain occupancy rates and types of treatment.
- Triage – area for mass casualty treatment.
- Ingress and Egress points for responding medical personnel.
- Post incident medical care.
- Trauma.

Security and Fire Protection

- total self-sufficiency may be required.
- Fire Dept. - inspect facility for hazards.
- Law enforcement – given drawings to show entrances and exits.
- Identification – ie. Colored arm bands.

Alert and Warning System

- outdoor as well as indoor (Individuals might be outside).
- Tested periodically.

Emergency Evacuation and Shelter-In-Place

- short term = less than 1 hour.
- Extended = more than 1 hour.
- Use of alternate exits and routes should be practiced regularly.
- Shelter-in-place – if evacuation if infeasible or undesireable.

Emergency Shutdown and Restoration

- assign specific responsibility for equipment shutdown.
- Plan should give priority to the facility structure after the emergency.

Business Continuity

- a comprehensive managed effort to prioritize key business processes, identify significant threats to normal operation, and plan mitigation strategies to ensure effective and efficient organizational response to the challenges that surface during and after a crisis.
- Organizational resilience – adaptive capacityof an organization in a complex and challenging environment.
- **BC plans and Continuity of Operations plans should NOT be part of the organization's emergency operations plan but should be maintained as separate plans**.
- **Objective is to resume critical functions as quickly as possible and to restore the business to its pre-emergency condition and location, or to a new location if necessary.**
- Business Impact Analysis (BIA)
    - Identify critical functions.
    - Assess the impact.
    - Determine the other elements of the business on which those critical functions depend.
    - Develop and prioritize recovery strategies.
- Vital records – those that are necessary to ensure the survival of a business.
- Arrangements to store vital records must be included in BC and COOP plans.
- Make arrangement for emergency funds at alternate operating sites.

CHAPTER 2 TERRORISM AFFECTING THE GLOBAL WORKPLACE

Terrorism

The Old Terrorists:

- practiced for millennia.
- Political motivations.
- Violence as a *didactic* tool (teaching or instructing).
- Traditional motivations.
- Showed discretion in means of attack and selection of targets.

The New Terrorists:

- religious fanaticism, supremacist ideology, or apocalyptic prophecy.
- Use of violence is less constrained and less didactic.
- Shock value.
- "Mass-mediated terrorism".
- Terrorist networks – recruiting followers and soliciting donations.
- US CFR (Code of Federal Regulations) – the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

- Domestic terrorism –occurs primarily in the territorial jurisdiction of the U.S.
- International terrorism – outside the US or transcends national boundaries. (must be a violation of criminal law in the US).

Approaches to Terrorism Analysis

It is the exploitation of emotions that allows the terrorists to succeed. The real targets are not always the actual victims.

- intent is to shock.
- That's why they target innocent civilians.

Multicausal Approach – terrorism results from several causes at once.
Political Approach – revolutionary ideas, radical groups.
Organizational Approach – rational, strategic course of action decided on by a group. Operational details are left to their lieutenants.
Psychological Approach – examines the terrorist's recruitment, personalities, beliefs, attitudes, motivations, and careers as terrorists. They don't care about alienating world opinion as they believe they are above it. Mujahideen – strugglers or holy warriors.

Winning the War on Terrorism

- lack of cooperation between law enforcement and intelligence work.
- Must use an all-hazards approach – multifaceted.
- The more the Russians tried to stamp out Islam, the more it grew as an act of ethnic, regional, and religious resistence.

State Sponsored Terrorism
- Transnational terrorism – across national borders.
- Funds, weapons, materials, and secure areas to conduct operations.

Counterterrorism Efforts
- modern intelligence + police methods + govt. sharing of information = Effective.
- US Dept. of State – travel advisories and warnings.

Chemical, Biological, Radiological, and Nuclear (CBRN) Terrorism
- dual use materials have a legitimate civilian application.
- Proliferation Security Initiative – global multilateral agreement to seize cargo.
- Generally, conventional weapons are the principal method with CBRN increasing.
- Superterrorism – the committing of violent acts using advanced technological tools to cause massive damage to poplulations and/or to public and private support networks.
- Chemical or Biological weapons – "the poor man's nuclear weapon".
- Nuclear power plants as attractive targets.
- Former Soviet Union – 40,000 to 80,000 nuclear weapons, poorly controlled.

Cyber Weapons
- vulnerable: telecommunications, energy, banking and finance, water systems, government operations and emergency services. (Modern industrialized Society).
- Most vulnerable – systems for a large number of users = educational institutions.
- Love bug virus.
- User friendly and abuser friendly.
- Essential infrastructures have shifted from mechanical or electrical to **electronic control**.

Conventional Weapons
- mass havoc.
- PGM – precision guided munitions.
- MANPADS – man portable air defense systems – can correct course in flight.

Asymmetric (between professional army and insurgencies) attacks and multiple simultaneous attacks may be expected.

CHAPTER 3 BOMB INCIDENT MANAGEMENT

- continue operating until it is determined that a hazard probably exists and that there is a legitimate need to evacuate all or part of the site.
- Bomb response is a management-level responsibility.

History

- China – 8th or 9th century.
- Europe – Gunpowder – 13th century.
- 1858 – Felice Orsini attempted assassination of Napoleon.
- Alfred Nobel – packaged explosives (dynamite) – 1866.
- Dynamitards – Irish revolutionaries.
- Bombings – preferred weapon of terrorists and a common tool for criminals.

Types of Bomb Incidents

Bomb – explosive or incendiary device designed to explode with force.
IED – Improvised Explosive Device.
Unattended item – not readily explained but could be a hazard.
Bomb threat – a bomb will or has been used.
Mail bomb – postal or courier system.
Post-blast – the scene after the bomb explodes.
Hoax – item or threat, not a hazard, but creates the impression.
Secondary hazards – on-site materials that are safe until affected by an explosion.

Elements of a Bombing

- Motive – criminal, political, personal.
- Material – main charge, initiator, triggering mechanism, safety switch.
- Knowledge – of bomb making, organization's activities, layout, and security.
- Opportunity – the element that the organization can control

Bomb Incident Management Plan

- limits the ability and plans for response.
- Unattended items, bomb threats, bombs, hazardous mail, post-blast.
- Most likely = **Unattended items**. Then threats, hazardous mail, bombs, post-blast.
- Plan should be based on:
    - Understanding the elements of a bombing.
    - Exposure of the organization.
    - Effectiveness of other emergency plans.
    - Current security measures.
    - Senior management recognition of the risk.

Bomb Security and Safety Considerations

Principles:

- Preventing a bomb from entering the site.
- Early detection of bomb incidents.
- Appropriate response measures.
- Careful design of facilities.

- Access Control – boundaries, identification, recording systems, restricting access.
- Defense-in-depth – additional levels to higher-value assets (control and access).
- Good workplace practices – keeping areas tidy so that items are quickly detected.
- Staff awareness – ability to detect and report.
- Training of supervisors and managers.
- Standoff distance – assets far from boundary or other security measures.
- Detection equipment – and trained staff.

Security measures chosen must be consistent with the organization's culture.

Bomb Risk Methodology

- appropriate prevention and response measures.
- Likelihood of incidents and potential consequences.
- Practice procedures.
- Establish a Threat Evaluation Team.

Bomb Threat Management Principles

- evacuation is NOT always best.
- May also lead to copycats.
- Threat Evaluation = procedures, planning, training, and rehearsal.

Bomb Threats

- develop a threat evaluation capability to determine correct response.
- Assessed by those with appropriate training and skills.
- TET – Threat Evaluation Team.
- Each site should have its own team.
- Small team can act more quickly that a large team.

- Threat evaluation consists of the 5 R's:
    - Receive
    - Record
    - Report
    - Review
    - Respond

- RECEIVE – system to capture any threats.
- RECORD – various threat checklists available (US Bureau of Alcohol, Tobacco, Firearms, and Explosives).

    - Checklist should be widely distributed and easily accessed.
    - Staff must be taught how to receive and record threats.
- REPORT – passed to the TET quickly.
    - All threats passed to a Threat Coordinator.
    - Threat Coordinator calls together the TET.
    - Threat Coordinator must have sufficient authority to evacuate site.
- REVIEW – most important and difficult.
    - Threat evaluation is a managerial decision making process.
    - The amount of time available for evaluating the threat can be calculated by subtracting the time required to evacuate the site PLUS a safety margin from the bomb deadline.
    - A perpetrator willing to kill is unlikely to provide a warning.
- RESPOND – if deemed feasible, measures must be taken to protect personnel and the business, including evacuation of all or part of the site.
    - Evacuate in coordination with the Chief Fire Warden.
    - Consider implementing the Business Continuity Plan.
    - (emergency personnel may require an evacuation without regard to financial and organizational implications.

<u>Identifying a Bomb</u>
- does not fit in environment.
- Security measures may increase the likelihood of detection.

<u>Responding to a Bomb</u>
- if the item is believed to be a bomb, initiate an immediate evacuation.
- Distance and Cover.
- More than one bomb may be on site – search egress routes and assembly areas.
- Only Emergency Services may classify as a Hoax.
- Evacuation assembly areas should be at least 300 meters (328 yards) from the building, not in line of site, not facing or under windows, behind solid cover.

<u>Suicide Bombers</u>
- recorded since late 19th c.
- very small subset of bombers.
- Move people away.

<u>Vehicle Bombs</u> (VBIEDs) – vehicle-borne IEDs
- detection is difficult particularly where public parking is provided.
- Forbid public parking on-site.
- Physically harden critical utilities.
- Use fences, bollards, trees, terrain, etc. to limit vehicle access.
- Pre-register drivers and vehicles.
- Detailed inspections.
- Isolation bay.

- Turnaround area.
- Harden site perimeter.
- Bombs in vehicles:
    - Secure garage.
    - Secure vehicle.
    - Search vehicle before use and after it has been unattended.

Off-Route Bombs
- used to attack vehicles in transit.
- Off Route Mines – shaped charged and explosively charged projectiles.
- Vary route and times, keep travel plans secure.

Unidentified items
- left unattended.
- Do not refer to a suspicious before it has been assessed. (Prejudices process)
- Does the item pose a hazard?
- Check video records (how it got there).
- If cannot be declared safe….EVACUATE.
- Not the role of management or staff to decide if it's a hoax. (Bomb Sqd)
- RECEIVE – received when it is found.
- RECORD.
- REPORT.
- REVIEW – may be obvious from witnesses or CCTV if accidently left behind.
- RESPOND – if hazardous, evacuate.

Post-Blast
Insurance may not cover the bomb damage.

Hazardous Mail
Includes bombs, noxious and poisonous materials, acids, chemical or biological agents, and needles and blades (called sharps).
- provides anonymity.
- Staff must be trained in identification and response.
- 4 elements: Motive, Material, Knowledge, Opportunity.
- disruption and ongoing fear.
- Affecting productivity.
- Company reputation.
- Litigation – especially if mgmt. failed to take appropriate measures.
- Normally designed to function upon opening.

Recognition of Hazardous Mail
Primary protection is recognizing it before it is opened.

Identification *"EXPLOSIVE PARCEL"*

E xcessive securing material
e X cessive weight
P rotruding wires or tinfoil
L opsided or unevenly weighted
O ily stains and discoloration
S tiff or rigid envelope
I s the package expected?
V isual distractions
E xcessive postage

P roper names and title incorrect
A ddress handwritten or poorly typed
R estrictive markings, e.g. "Confidential"
C ommon words misspelled
E ither unusual or foreign origin
L acks address of sender

- the whole device is often mounted on a piece of card or wood and then heavily taped or tied to stop it from coming apart.

Investigation

- if arrived through mail – unlikely to have time switch. (time to gather info and assess).
- Transparency sprays.
- Metal detectors – handheld wands are NOT designed for mail screening.
- Explosive vapor detectors – expensive and must be trained.
- Explosive detection sprays. (Detectors and sprays used as secondary screening tools).
- X-ray machine – better to screen before entering the mail center.

Response

- apply isolation measures if deemed hazardous.
- Do not move item and evacuate, if it can't be determined it was delivered by mail.
- If deemed hazardous:
    - Do not open.
    - Do not wet.
    - Do not place in a container.
    - Consider moving item to isolation area.
    - Primary protection is distance.

Chemical and Biological (CB) "White Powder" Incidents

- more likely to be a hoax.
- Danger that it may enter the building's airflow systems. (Separate the mailroom from the site's air conditioning or other circulation system.
- Usually will not be detected until item is opened.
- Limit distribution of the material.
- Look after any staff exposed.
- Specifically designed containment cabinet.
- Sealable box or bag.
- If exposed:
    - Leave the contaminated area.
    - Do NOT join the general population.
    - Wash hands AND trap water for analysis.

Courier Delivered Items

- could be fitted with a time fuse or anti-handling switches armed by courier
- if there is any indication that the item is hazardous…DO NOT HANDLE….EVACUATE. Treat as a bomb place on-site, not as a mail bomb.

SEARCH

Reasonable belief bomb on-site + Adequate Time = Try to find.

- searches may be conducted before, during, or after an evacuation.
- Searching is a skill that can be taught to staff.
- Look for that which is out of place.
- Keep areas tidy and restrict the public to public areas.
- Use of replica bombs is NOT recommended.
    - Could be illegal.
    - May be left behind after training.
    - Could be found by someone not involved in training.
    - Bombs have many different appearances.
- Central Search Coordinator – remains in crisis control center but decides where and in what order to search, and when to evacuate.
- Search Supervisor – for every 3 or 4 two-person teams.
    - Communications link back to Coordinator.
- Emergency Response Packs should be available on each floor (floor plan, flashlight, mirror, tape to mark areas of items found, pens, paper, chalk, labels, gloves, search instructions, and communication instructions).
- Radio and cell phone use should be avoided.

Types of Search

Occupant Search – all staff trained. External areas and engineering searched by nominated teams.
Warden search – trained fire wardens canvass for out of place items.
Team Search – Trained teams. Higher level of training required.
High-Risk Search – trained government personnel.

Search Techniques

- teams of 2 people.
- Leave at least one vacant room or area between each team member.
- Utility and engineering spaces are best searched by those who work there.
- Mark the door after a room has been searched.
- Use CCTV where possible.
- Specific skills are required to search cars, trucks, aircraft, watercraft, outdoor areas, and people.
- Tools:
    - Mirrors
    - Explosive vapor detectors
    - Nonlinear junction detectors – detect concealed electrical circuits.
- If found:
    - Do not touch
    - Inform supervisor
    - Get as much info as possible
    - Digital photographs
    - Mark location
    - Be available as a witness to emergency responders.

Explosives and Explosive Effects

May be Mechanical, Chemical, or Nuclear.

- Mechanical – explosion result of a buildup of heat and pressure inside a vessel.
- Chemical – chemical composition whose bonds can be broken easily, causing the material to become a gas very quickly.
- Nuclear – either the fission or fusion of atomic nuclei under extraordinary pressure.

- explosive items are assigned to compatibility groups that indicate which items may be stored or transported with which others ("Orange Book" – United Nations – *Recommendations on the Transport of Dangerous Goods*).

- High and low explosives, depending on their velocity of detonation (VoD), which is the speed of the chemical change over a linear distance. (Standard measure for explosive comparison is TNT (trinitrotoluene), which has a VoD of 6,900 meters (22,600 ft.) per second).

- most explosive devices consist of a detonator or igniter.

Explosive Effects

Blast
The rapid expansion of gas (the blast wave) breaks and destroys surrounding structures and people. Can be thought of as a wall of compressed air travelling close to the speed of sound. Immediately behind the blast wave is a low-pressure area from which the compressed air was drawn. This low-pressure area (incorrectly called a vacuum) further damages structures weakened by the blast wave by causing them to stress in the opposite direction.

Blast is applied to an object either (1) through the sudden increase in pressure (peak incident pressure) that passes through the object, or (2) by applying pressure increasingly until the object fails or the blast is reflected (peak reflected pressure).

The nature of the blast wave depends on several variables:
- Type of explosive and method of detonation. (The rapidity with which an explosive develops its maximum pressure is a measure of its ***brisance***.
- Location – reflecting surfaces, proximity of combustibles, etc.
- Packing or Confinement.

Kilopascals - pressure measurement unit.

Distance provides a significant benefit.

Fragmentation – fragments projected from the blast.

Heat – the detonation process is **exothermic** and generates considerable heat. Unlikely to start a fire unless specifically designed as an incendiary or near combustibles.

Blast Impulse – the time during which pressure is applied to the body.

Emergency Management Considerations for Bomb Incidents
- Shelter
- Data search – bring access control and visitor records to assembly area.
- Assembly areas.
- Special item removal – information, equipment, laboratory samples, etc.
- Alerting of neighbors.
- Shutdown procedures.
- Security.
- Emergency rendevous point (ERV) – to brief responding services.

Reoccupation considerations:
- decision, search, clients and customers.

Blast Protective Design Considerations

May assist in deterring, detecting, and responding to bombs as well as reducing the effects of an explosion.

CPTED – Crime Prevention Through Environmental Design.

- critical assets and functions should be separated from public areas and protected by at least two walls (that is, they should not border public areas).
- Films and other technologies to reduce glass fragments.
- Trash bins – if situated correctly, special bins can direct a blast away from people.
- Cloakrooms – should not be established near utility lines or other critical assets.