



Incident Management Plan Assessment

Deidrich Towne, Jr., CBCP, MBCI

Peter R. Laz, MBCP

David H. Ziev, MBCP, MBCI

*Private & Public Businesses, Inc.
St. Louis, MO*

Email: ppbi@twcny.rr.com



AGENDA

- Introductions
- Module 1 – Incident Management Planning Basics
- Module 2 – Incident Management Plan Components
- Module 3 – PPBI Maturity Model Overview
- Module 4 – Assessing Your Plan
- Module 5 – Review and Conclusions



Introductions

- We learn best when we share backgrounds and knowledge.
- Share with each other...
 - Your Name
 - Position/Role
 - Level of Incident Mgmt Plan experience
 - Exchange business cards



Module I

Incident Management Planning Basics



Power Outage **Civil unrest** **Hurricane**
Fire **Software** **Terrorism** **Tornado**
Construction **Pandemic** **Earthquake**
Accident **Flood** **Telecom**
Data Center Move **Explosion** **Privacy Exposure**
Cyber Security





What is an Incident Management System?

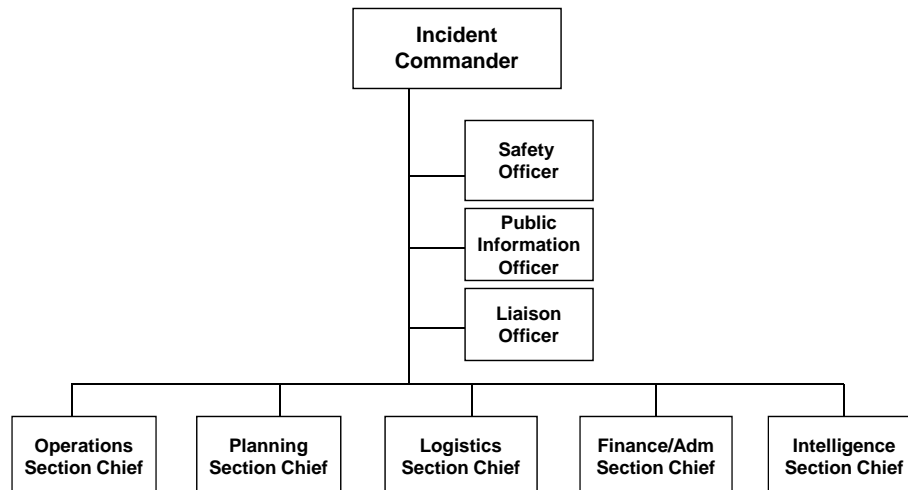
An integrated set of processes, tools and responsibilities that allow effective, efficient and economical management of any event that could (or does) impact normal business operations.

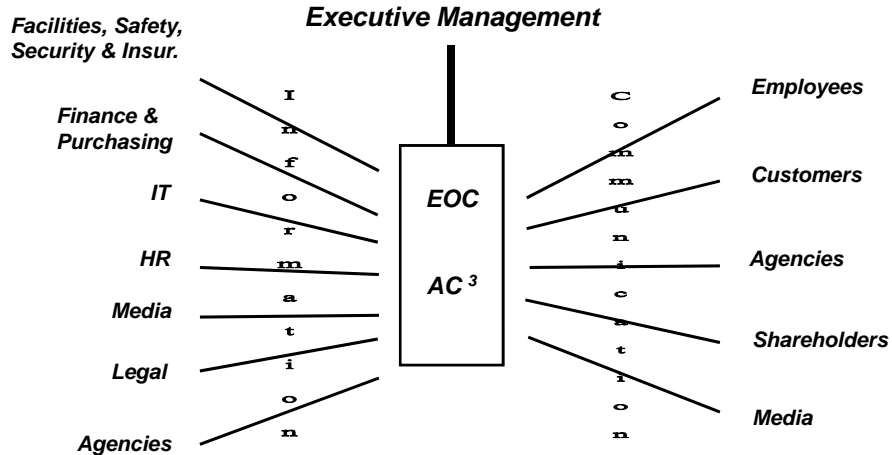
AC³

- Assemble the decision makers
- Coordinate response, recovery & restoration efforts
- Collect all incident related information
- Channel communications appropriately

- Emergency Operation Center and Infrastructure
- Documented Procedures and Guidelines
- Emergency Management database & recovery plans
- 24 x 7 Instant Meeting Line
- Training / Rehearsal drills

- Outlined in the plan
- Solidified during Planning & Exercising





Why do Incident Management Planning?

- Effectively, Efficiently and Economically manage all aspects of a disruptive event throughout its lifecycle
 - Links Technology Recovery and Business Recovery
 - Enhance alignment - Private and Public Sectors
 - Follows BC/DR Professional Practices
 - Enhanced Life Safety; No additional staff required
 - Protects company value; Prudent Management



The Quick Test

- What will happen when your people are required to operate during a disaster?
 - Use the telephone and signature test



Module 2

Incident Management Maturity Model Overview



The Dimensions of the Plan - AC³

- **A** - Assemble the Decision Makers
- **C** - Coordinate Response, Relocation and Restoration Efforts
- **C** - Collect all Incident-related Information
- **C** - Channel Incident-related Communication



Incident Management Maturity Model

- Level 1 = Inadequate
- Level 2 = Marginal
- Level 3 = Acceptable
- Level 4 = Outstanding

Refer to the handout containing the PPBI Incident Management Maturity Matrix.

Private and Public Businesses, Inc.

Revised: August 2009



<i>Functional Category</i>	<i>Level 1 Inadequate</i>	<i>Level 2 Marginal</i>	<i>Level 3 Acceptable</i>	<i>Level 4 Outstanding</i>
Assemble	Inadequate notification process.	Limited / outdated contact information.	Expanded contact information updated within 12 months.	Comprehensive contact information with automated process and response capabilities updated monthly.
Coordinate	"Just in time" assignments; in-house only.	Emergency responsibilities pre-assigned with limited training. Coordination with appropriate emergency staff of opposite sector.	ICS organization implemented. EOC equipped. Cross section leadership briefings.	Functionally exercised command system within 6 months. Defined interrelationships between command staff and tactical operations. Cross sector stakeholders involved during rehearsals.
Collect	Limited staff to handle incoming calls (ad-hoc).	Staff trained in situation monitoring. I/P from multiple sources.	Incident Action Plan process utilized. Documentation system in place.	Electronic version of action plan and documentation system.
Channel	Timely information not shared with appropriate stakeholders.	Information disseminated/released upon request at irregular intervals.	Communicating to selected stakeholders regularly; PIO established.	Announced / scheduled media briefings to multiple stakeholders. Publicize known information. Trained PIO staff.

Private and Public Businesses, Inc.

Revised: August 2009



The Drill Starts Now





- Friday, 4:00 p.m.
- Corporate Security receives a call from an extension telephone inside the data center.
- An estranged husband of a secretary in the IT department has taken his wife and three Data Center Control Room employees hostage in the Data Center.



Immediate Steps

- What would you do first given this information?

- _____
- _____
- _____



- He reportedly has a gun, and a dirty bomb is strapped to his torso.
- Two of the employee hostages have access to classified information and the ability to fully disable IT Services.
- Local law enforcement has been alerted via 9-1-1 and they are expected in 3-4 minutes.



IT Operations Threatened

- How does this additional information pose a threat to the IT/IS operation?
- _____
- _____
- What steps become more important with this new information?
- _____
- _____



- A gunshot is heard from within the data center.
- In a second call from the phone inside the data center, we learn that one of the two IT analysts with extensive knowledge of IT Services has been wounded.
- Law enforcement directs an evacuation of the facility and establishes an inner perimeter around the entire facility.



Panic Sets In

- What steps must be taken upon the receipt of this new information?
 - _____
 - _____
- Who is in charge of the scene; the facility?
 - _____
 - _____



- The CEO is demanding that the IT Services be protected to avoid any interruption of business.
- Local TV and radio stations have learned of the incident via police radios. They have set up outside the facility and are requesting an interview with the CEO or CIO.
- Live pictures of the facility are now being broadcast on local TV stations.



What Staff Is Needed?

- How do you protect IT Services under these conditions?
 - _____
 - _____
- Who addressed the media concerns?
 - _____
 - _____



- It's now 4:45 p.m., almost time for the local TV news.
- The estranged husband has offered to release the three IT analysts in exchange for ...



Decisions

- On what information can you base decisions at this point?
 - _____
 - _____
- Who has the authority to make these decisions?
 - _____
 - _____



Debrief

- Discuss the entire incident.
- What lessons might you have learned?
- _____
- _____
- _____
- What steps will you take going forward?
- _____
- _____



Do you have an Incident Management Plan?

- What would you like to see included in an Incident Management Plan?
- Who would author the plan in your organization?
- How would the chain of command differ from the chain used in normal business?
- Let's examine some recommendations.



Module 3

Incident Management Plan Components



Common Elements of An Incident Management Plan*

- Functional Roles and Responsibilities
- Lines of Authority shall be established.
- Direction, Control, and Coordination
- Communications and Warning
- Operations and Procedures
- Logistics and Facilities
- Training
- Exercises, Evaluations, and Corrective Actions
- Crisis Communications, Public Information
- Finance and Administration

* (NFPA 1600, 2007 Edition, Section 5)



Functional Roles and Responsibilities

- Identify the functional roles and responsibilities of the following during Mitigation, Preparedness, Response and Recovery:
 - Internal and External Agencies
 - Organizations
 - Departments
 - Individuals



Laws & Authorities

- The disaster/emergency management program shall comply with applicable legislation, regulations, directives, policies and industry codes of practice.
- The entity shall implement a strategy for addressing needs for legislative and regulatory revisions that evolve over time.



Direction, Control, and Coordination

- Develop the capability to direct, control, and coordinate response and recovery operations.
- Utilize an Incident Management System.
- Identify specific organizational roles, titles, and responsibilities for each management function as specified in the Emergency Operations Plan.

Cont'd

Page 33



Direction, Control, and Coordination

- Determine the level of implementation of the plan according to the magnitude of the incident.
- The Incident Management System shall be communicated to and coordinated with all stakeholders.
- Established procedures for coordinating response, continuity, and restoration while complying with applicable regulations.

Page 34



Communications and Warning

- Communications systems and procedures shall be established and regularly tested.
- Develop and maintain a reliable capability to alert officials and emergency response personnel.
- An emergency communications and warning process/procedure shall be developed and periodically tested to alert customers or citizens of an actual or impending emergency.



Operations and Procedures

- Develop, coordinate, and implement operational procedures to support the Incident Management Plan.
- Particular attention shall be paid to considerations of life safety.



Operations and Procedures

- Standard Operating Procedures are developed for identified credible hazards.
- Situation Analysis is conducted to include damage assessment and resources needed. Established procedures for maintaining continuity of response via the Incident Management Plan.



Logistics and Facilities

- The organization shall establish procedures to locate, acquire, distribute, and account for services, personnel, resources, materials, and facilities procured or donated to support the response to the incident.
- A facility capable of supporting response and recovery operations shall be established, equipped, periodically tested, and maintained.



Training

- The organization shall perform an assessment of training needs, develop and implement a training/education program to support the Incident Management Plan.
- Personnel shall be trained in the organization's incident management system.
- Training records and documentation shall be maintained.



Exercises, Evaluations, and Corrective Actions

- The Incident Management Plan shall be evaluated through periodic reviews, testing, after-action reports, and exercises.
- Exercises shall be designed to test individual essential elements, interrelated elements, or the entire plan.
- After-action or lessons learned debrief sessions shall be conducted to ensure that corrective action is taken on any deficiency identified.



Crisis Communications, Public Information

- The organization shall develop procedures to disseminate and respond to requests for pre-disaster, disaster, and post-disaster information, including providing information to the media and to deal with their inquiries.
- Where the public may be impacted by a hazard, a public education program shall be implemented.



Finance and Administration

- The organization shall develop financial and administrative procedures to support the Incident Management Plan before, during, and after an emergency or a disaster.



Module IV

Assessing Your Plan



PPBI Incident Management Plan Assessment Tool

- Use the tool to evaluate your organization's Incident Management capabilities.
- Take 15 minutes to assess your plans against the common elements of an Incident Management Plan

Assessment Tool Discussion

- How did you do in each of the categories?
- What improvements would you like to see?
- How would you propose to make those improvements?
- Take these lessons learned and apply them to our next exercise...

Drill #2 Starts Now





A Secure Facility

- Your organization has a secure facility with multiple servers in your data center.
- Tailor this to your own organization's data center.
- You have an Incident Management Plan and tried and proven BCP/DRP's.
- You have trained your staff to use the plans.



A Monday Holiday

- Just outside your facility there is a road or driveway.
- A large tanker truck is near the entrance to your facility; not sure why.
- It is Monday morning at 9:00 a.m.
- It's a holiday, so in IT, only maintenance staff is present, conducting improvement updates to several systems.

Notification & Response



Notification & Response

- **May 25, 2009:** At 0930 hours EDT, the Sheriff's Department, Prepared County, New York reported an explosion at a multiple vehicle accident on Hoefler Avenue at E. Main Street. State Police, fire, and EMS are responding to the scene.



Notification & Response

- **May 25, 2009:** 0935 hours, EDT, NYSP report that an explosion in a tanker truck has caused two other vehicles to collide – a tour bus, and a passenger car owned by Your Company.





Chemical Identified

- The tank truck involved in the accident in Ilion was believed to be filled with Liquid Hydrogen, ID # 1966.



EXPLOSION!

- Fire departments are now fighting furiously to contain the blaze to the truck.
- There are multiple injuries reported amongst passengers in the two other vehicles. At least one of the drivers in the other vehicles was believed to have been fatally injured.
- Evacuation in the area as far away as 1 mile has been advised.

Private and Public Businesses, Inc.

Revised: August 2009



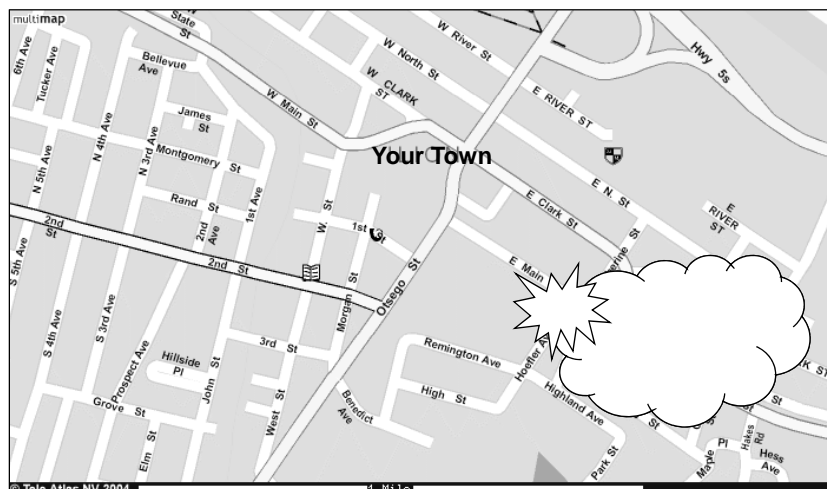
- **May 25, 2009:** 0950 hours, EDT. Prepared County Fire Control reports that seven fire departments have responded to the scene. The rapidly developing situation gave no warning or evacuation time to area residents.
- “You could see the red fire boiling over ... like a volcano,” said Rose Schott, 31. Schott had been awakened in her home, on Spring Street .”



Page 57

Private and Public Businesses, Inc.

Revised: August 2009



Page 58

- **May 25, 2006:** At 0950 hours EST, FBI officials reported that WUTR Television received a phone call at its home office in Utica from someone claiming to be a member of AlterNOT. The caller claimed credit for AlterNOT for exploding the tanker truck. The caller said that other such bombs are being planted in chemical tankers, but didn't say where.



Media Coverage



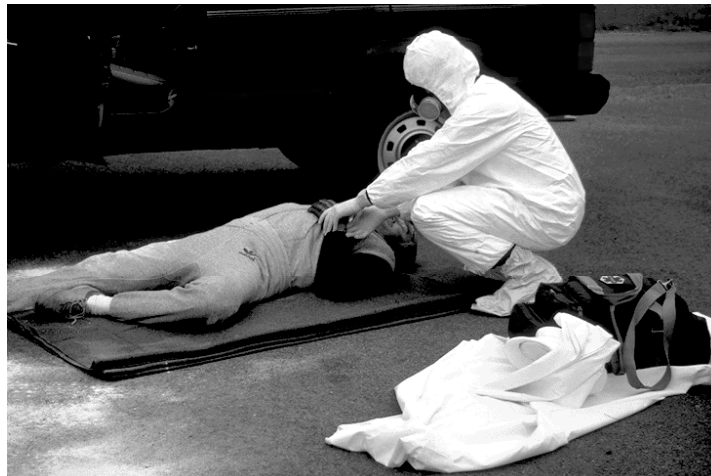


Media Relations

- **May 25, 2009:** 1030 hours EDT Elaine Houston, TV news reporter from WNYT-TV13, has reported on the tanker truck explosion incident with a live interview of the Prepared County Sheriff. She has announced an interview with a HazMat expert to be aired as part of the noon broadcast.



Casualties Reported





Your Plant & Data Center are Impacted



Page 63



Your Company Offers Assistance

- Justin Tyme, Plant Security Supervisor, at Your Company has offered full cooperation to the Prepared County Office of Emergency Services.
- Your Company has 80 employees on the holiday shift, many of whom were affected by the smoke from the explosion and fire.

Page 64



The Problem

- **It is the first hour of response.**
- **Based on the preceding representative events, consider what actions and decisions you would be making during this period.**
- **Discuss your actions with the class.**



Module V

Review and Conclusions



Not a Question of If, but When...

- Business and the Government are placing greater emphasis on being prepared.
 - <http://www.ready.gov/business/index.html>
 - Includes a Crisis Communications Plan
- Your customers will demand resiliency.
- Your shareholders will depend on it.
- Our enemies know how much it matters to us.



We All Have Plans

- Have we evaluated them against standards?
- Can the PPBI Incident Management Assessment tool help you evaluate your plan?
- Have you exercised your plan in real time?



Discussion

- How do you feel your plan will fare in light of the considerations of the Incident Management Maturity Model from PPBI?
- What are the strengths of your plan?
- What are the areas for improvement?
- How would you create an Improvement Plan?



It's Important to.....

- Have a plan.
- Assess your plan against approved standards.
- Practice or exercise your plan in real time with your employees participating.
- Understand that fear, time, and quality will be issues during a disaster.



Who has the next question?

- Please complete the evaluation form for this course. We take your comments very seriously to improve our courses.
- Please visit our website at PPBI.Org, and keep in touch via e-mail to:

PPBI@twcny.rr.com