

**March 11, 2009**

# Crisis Management Planning

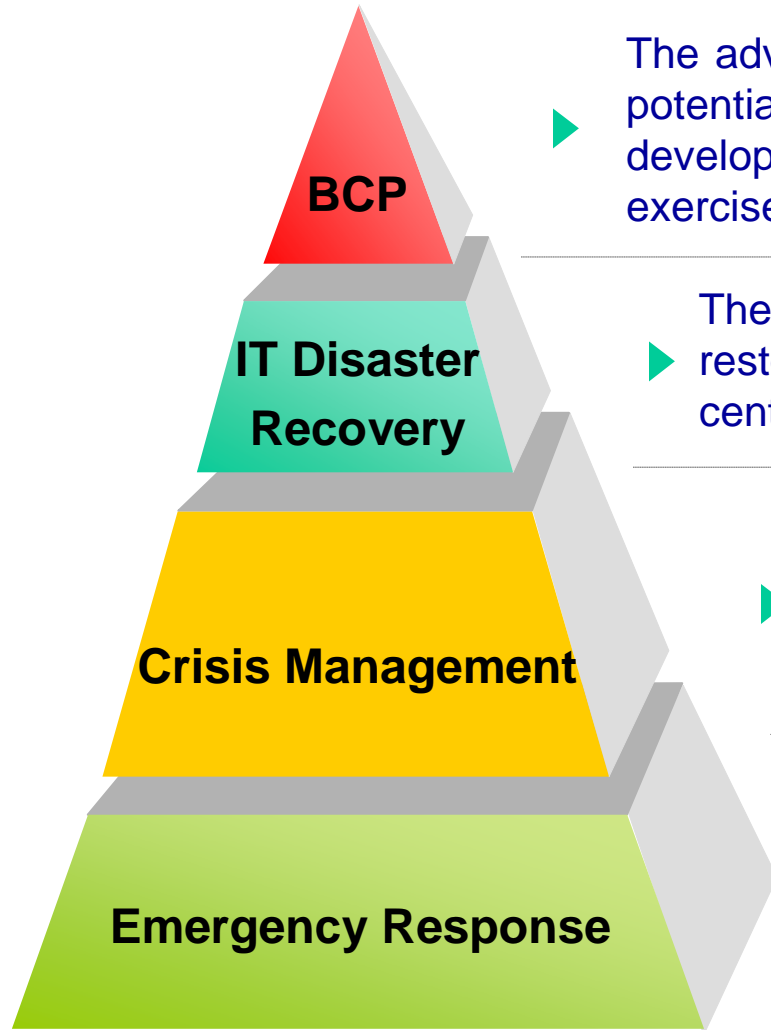


## Business Continuity Management

**Tony Adame—Senior Vice President**  
West Region—BCM Practice  
949.399.5962

- Business Continuity Management - Defined
- “Crisis” Defined
- Some Basic Facts
- Why do We Prepare?
- Workplace Violence – Some Stats
- 8 Steps for Crisis Management Preparedness
- The Risk Assessment
- Crisis Management Team Membership
- The Event
- Crisis Management Activation
- How not to Develop a Preparedness Program

# Business Continuity Management



▶ The advance preparations necessary to identify the impact of potential business interruptions; formulate recovery strategies; develop business continuity plans; and administer a training, exercise and maintenance process.

▶ The technological piece of a continuity plan. Focus is on restoration, possibly at an alternate location, of data center services and computer processing capabilities.

▶ An organization's ability to strategically manage the internal and external communications after an event in order to protect its reputation and brand image.

▶ An organization's coordinated, effective and timely response to an emergency. The goal is to avoid or minimize injury to personnel and or damage to company assets.

# *Crisis*

*Any situation that is threatening or could threaten to harm people or property, seriously interrupt business, damage reputation or negatively impact share value.*

**Most organizations will face a crisis every 4 - 5 years**

***All Unplanned Events Are  
Not Emergencies***

***All Emergencies Do Not  
Become Crises***

***All Crises Are Emergencies***

# Why Preparation is Important

- Increased regulatory and self-regulated requirements
- Pressure from senior management or Board
- Pipeline sustainability and delivery
- Reliance on single and sole source vendors
- Product quality
- Strategic alliances
- Inquiries from customers
- Cost of insurance and insurance carrier requirements
- Perceived as competitive edge
- History of events (vulnerable industry)

# Reasons Companies Do Not Prepare

- Denial
  - “It’ll never happen here!”
- Lack of Awareness
  - “Risk? What risk?”
- Ignorance of Warning Signs
  - “We all thought that she was a bit eccentric!”

# Types of Workplace Violence

Workplace violence is identified by the following types:

- Employer directed - violence against workplace authority: supervisor, manager, director\*.
- Domestic directed - partner or would be partner engages in violence against the object of his or her affections.
- Property directed - acts against any property that the company/employer owns.
- Commercial directed - an employee participates in events against the company that can include theft of money or property and may also involve violence.

\* According to studies by the National Safe Workplace Institute in Chicago, the most dramatically increasing type of workplace violence is employer-directed.

In the early 90's, there was an average of one employer-directed homicide per month in the United States. Recently that has escalated to an average of five or six monthly.

# Background Statistics

- Homicide is now the second highest cause of work-related death in the United States.
- National Institute of Occupational Safety and Health - homicide accounted for 12% of job-related deaths.
- Approximate rate is .7% homicides per 100,000 workers.
- U.S. Bureau of Labor Statistics - homicide was the leading cause of death for women at work, (42% of on-the-job fatalities).
- Justice Department – one-sixth of all violent crimes in the US occur in the workplace.
- American Management Association - surveyed 500 companies and nearly one-fourth stated that a minimum of one worker had been attacked or murdered on the job since 1990. Almost one-third stated that a violent incident has occurred more than one time.
- National Institute of Occupational Safety and Health - guns account for 75% of workplace homicide deaths.
- The Brady Center to Prevent Gun Violence estimates each workplace homicide costs employers between \$250,000 and \$1,000,000
- Some cases of serious injury or death involving employer negligence have led to jury awards averaging \$3,000,000

# Workplace Violence Sample Policy Statement

The safety and security of *Company* employees is of the utmost importance to *Company*. *Company* has adopted a Zero Tolerance Policy for workplace violence.

Acts or threats of physical violence including intimidation, coercion, and/or harassment, which involve or affect *Company* employees, visitors, guests or other individuals will not be tolerated. Violations of this policy will be investigated by *Company* "*Department*". Violations of this policy may lead to disciplinary action including dismissal, arrest, and prosecution.

**NOTE:** *Harassment of a sexual nature should be addressed under the organization's sexual harassment policy.*

# Warning Signs of Possible Violence

- Excessive feelings of rejection, persecution, or victimization
- Social withdrawal
- No strong, positive peer support group
- Feelings of isolation, being friendless, or alone
- Expression of violence in writings and drawings
- Frequent, intense and uncontrolled anger expression
- Past pattern of impulsive and chronic intimidation and other verbal and physical aggressive behavior
- Drug and alcohol abuse
- Unusual interest in Workplace Violence incidents
- Habitual and unexplained absenteeism
- Frustration with substandard work performance
- A past history of violent or aggressive behavior
- Inappropriate access to and use of firearms
- Intense prejudice and intolerance for differences (can be based along ethnic,, ability, physical appearance, sexual orientation, gender)
- Willingness to victimize individuals with an identifiable difference
- Affiliation with anti-social or "hate" groups
- Specific and detailed threats to use violence

# The 8 Steps of Crisis Management Preparedness

## 1. Identify Your Crisis Communications Team

- A small team of senior executives
- Ideally, the team will be led by CEO

## 2. Identify Spokespersons

- Only ones authorized to speak for the organization
- CEO should be one of those spokespersons, but not necessarily the primary spokesperson.
- Decision about who should speak is made after a crisis breaks — but the pool of potential spokespersons should be identified and trained in advance.

## 3. Spokesperson Training

- Training teaches how to be prepared to respond in a way that optimizes the response of all stakeholders.

## 4. Establish Notification Systems

- Need means to reach our internal and external stakeholders using multiple methods.
- Must pre-establish notification systems that will allow to rapidly reach stakeholders
- Multiple vendors available to contact stakeholders in a pre-established database
- Technology can be triggered with a single call or email.

# The 8 Steps Continued

## 5. Identify Key Stakeholders

- Who are the key internal and external stakeholders
- Need to ensure that they receive the messages you would like them to repeat elsewhere.

## 6. Perform Risk Assessment

- Brainstorm on events which can impact your organization.
- Some may be preventable by modifying existing methods of operation.
- Determine possible responses and expected resource needs
- Don't forget about scheduled crisis e.g., reductions in force, IT upgrades, financial disclosures

# The 8 Steps Continued

## 7. Develop Holding Statements

- Designed for use immediately after a crisis breaks — can be developed in advance to be used for a wide variety of scenarios
- Review holding statements on a regular basis to determine if they require revision and/or whether statements for other scenarios should be developed.

## 8. Training and Drills

- Develop scenario based exercises (based on a known peril) and evaluate adequacy of existing plans and communication mechanisms
- Update plans as required

**Management's response can help contain, or just as likely exacerbate the magnitude/seriousness of, a situation!**

# Risk Assessment

What can hurt you, and what is the possible impact?



**Organizations should plan for frequent and high impact threats! Plans must be specific to the threat, site, IT infrastructure, operations, & people.**

# Have you planned for a Workplace Violence Incident???



# Crisis Management Team Members

“Illustrative”

- Team establishes policy
- Internal participants set strategic vision for addressing event
- Coordination with Emergency Response and Business Continuity teams
- Communicate with staff, public, regulators, & other stakeholders

Possible Team Members	
C-Suite	Legal
Human Resources	Information Services
Public Relations	Regulatory Affairs
Risk Management	Operations
Facilities	Security
Finance	Others As Needed
<b>Emergency Response Team</b>	
<b>Business Recovery Team</b>	
<b>Outside Agencies &amp; Resources</b>	
Police, Fire, Medical, Hazmat, Emergency Mgt., Public Works	Contractors & Vendors

# Training, Drills & Exercises: Keys to Success

- Training:
  - All Team members
  - Others as may be necessary
- Exercises:
  - Practice specific skills
  - Familiarization of plans
  - Validation
  - Identify deficiencies
  - Update Plans as required



- Do's
  - Take all threats seriously
  - Try to be calm
  - Listen with empathy
  - Reassure the person
  - Call 911 as soon as possible
  - Document as much as you can after the event
  
- Don'ts
  - Confront an angry person
  - Threaten, dare, or criticize
  - Bargain
  - Make any physical contact
  - Take any challenging stances
  - Invade his/her personal space

# Crisis Management Activation

- Quickly and Accurately Assess The Situation
- Consider the Current and Future Impact on the Company, its People, Operations, Public Image, and Financial Position
- Ensure Initial Emergency Response Efforts are Progressing e.g. Protection of Life, Property, Equipment
- Once Able – Allow for Business Continuity Process to Begin
- Closely Monitor Situation
- Prepare for On-Going Crisis Management Activities
- Communicate, Communicate, Communicate

# How **NOT** to Develop a Preparedness Program

*Dilbert: By Scott Adams*

