

3 Phases of Every Incident

Mark Alley
Senior Director
Emergent BioSolutions

Variety of Incidents

- Embezzlement
- Sexual Harassment
- Racial Discrimination
- Criminal Incident
- Fire
- Severe Thunder Storm
- Tornadoes
- Severe Winter Storm
- Workplace Violence
- Terrorism
- Bomb Threat
- Civil Unrest
- Suspicious Mail
- Power Outage
- Flooding
- I.T. Hacking
- Injury or Death of Staff
- Sexual Assault

Minor Incidents vs. Crisis



Minor Incidents

- A “minor incident” is an event or series of events that causes a disruption of normal operating procedures
- The potential negative consequences of a minor incident are manageable, temporary, and not severe
- Example – a staff member slips and falls, twisting their ankle

Crisis

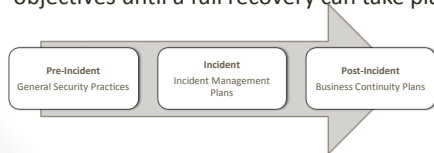
- A crisis is an event or series of events that causes a disruption of normal operating procedures and has resulted or is substantially likely to result in a negative consequence
- Potential negative consequences include:
 - Death or significant threat to life
 - Substantial damage to reputation, credibility, or public standing
 - Adverse financial impact

Risk-Assessment Matrix

PROBABILITY OF OCCURRENCE	SEVERITY OF CONSEQUENCES			
	NEGLIGIBLE	MARGINAL	CRITICAL	CATASTROPHIC
Likely	Tripped by uneven terrain			
Possible			Hit by bicycle courier	Killed by car
Unlikely		Mugged		Murdered
Rare			Raped	

3 Phases of an Incident

- **Pre-Incident:** Preparations and training before an incident occurs
- **Incident:** Actions and directions after an incident has occurred in order to manage the incident and bring it under control
- **Post-Incident:** Actions taken to minimize the impact of an incident on overall business objectives until a full recovery can take place



{ 7 }

General Security Practices

- The pre-incident is the time when things are going well, but it is understood that a negative situation could happen
- General Security Practices should be implemented at all sites to educate employees about what their roles and responsibilities are before and during an incident
- General Security Practices include instruction for what employees are expected to do during a fire, severe weather, a bomb threat, active shooter, protestors, and so on

{ 8 }

Incident Management Plans

- Incident Management Plans (IMPs) are used when an incident is actually occurring that is of the size and scope that requires managing
- IMPs provide structure to the people managing the incident and provide checklists of items that generally need to be accomplished during specific incidents
- Three goals for every incident:
 - Life Safety
 - Incident Stabilization
 - Property Conservation
- IMPs have pre-approved media statements

{ 9 }

Incident Management Plans Example – Serious Injury or Death

- Provide immediate medical attention
- Collect all additional information from police, hospitals, family members and witnesses
- Implement the incident communication chain (telephone tree)
- If the Head Librarian deems it appropriate, they will contact the designated legal counsel
- The Head Librarian will contact the insurance agent within a reasonable period of time

{ 10 }

Incident Management Plans Example – Serious Injury or Death

- In the event the library is contacted by the media, all questions are referred to the designated spokesperson
- All library personnel involved will thoroughly document their actions
- The Head Librarian or designee will follow up with the victim's family to offer support

{ 11 }

Incident Management Plans

- An IMP should include an Incident Communication Chain that indicates names and contact information of people who need to be called and who is responsible for making the call(s)



{ 12 }

Business Continuity Plans (BCPs)

- Business Continuity Plans (BCPs) are used when the incident is stabilized, and decisions need to be made on how to keep the organization functioning while work is done to get back to normal operations
- BCPs contain pre-populated recovery strategies and information necessary to make informed decisions



{ 13 }

Business Continuity Plans (BCPs)

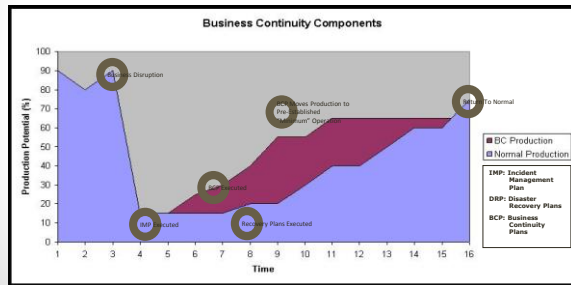
- Information contained within the BCPs can be used to develop interim recovery guidelines and procedures for operating between the “time of disaster” and the recovery back to “normal operations”
- At this stage, it doesn’t matter what happened. The key is getting back operational as soon as possible



{ 14 }

Utilizing Plans to Minimize Impact

Lack of Business Continuity Plans could impair the organization’s ability to maintain critical operations following a significant disruption



{ 15 }

Camping vs. Home



Business Continuity Methodology

- Identify critical functions – what are the critical functions necessary to operate
 - Generally 6 – 12 functions
 - Examples – process payroll, check-in and check-out books, record keeping
- On Site Relocation – having a plan in place that allows you to move critical functions to another location on-site if the current location is not accessible
 - This may mean displacing other non-critical functions
- Off Site Relocation – having a plan in place that allows you to move your critical functions to another location off-site
 - Minimum required space
 - Accessibility considerations
 - Cost considerations

{ 17 }

Business Continuity Methodology

- Contract Services – what / who are the contract services you could call in to perform the critical functions
 - Temporary service for payroll & accounting
 - Temporary help servicing customers
- Other contract services you may need following a critical incident
 - Security
 - Construction
 - Public Relations Expert
 - Accountants
 - Restoration after smoke or water damage
 - Hazardous Material clean-up / removal
 - Legal
 - Information Technology

{ 18 }

Business Continuity Methodology

- Critical Equipment – what equipment is needed to operate your critical functions
 - All critical equipment is listed including the vendor, cost, and estimated time for replacement
- Disaster Recovery - is the process, policies and procedures that are related to preparing for recovery or continuation of technology infrastructure which are vital to an organization
 - The ability for the site to operate its critical functions if technology is lost
 - The process in place to recover the lost technology

(19)

Crisis Communications Fundamentals

- Employees, customers, stakeholders and public safety are equally important
- Candid, accurate, and timely communication with key stakeholders and other principal audiences is critical
- Every effort must be made to minimize the negative impact of a crisis on the organization's reputation
- Advance planning and training will lead to crisis communications readiness

Crisis Communications Goals

- Foresee potential crisis situations and prepare for them
- Develop response strategies and principal messaging
- Initiate response rapidly
- Quickly gather information and assess the situation
- Make prompt decisions based on sufficient information

Crisis Communications Goals

- Reach out proactively
- Communicate with employees, customers and the general public through the media
- Communicate approved key messages
- Speak publicly through a single spokesperson, if possible
- Prepare thoroughly and speak consistently to all audiences
- Assume the worst and plan accordingly. As the crisis unfolds, identify the worst-case scenario and prepare for it

Media Relations Fundamentals

- The rights of the media:
 - First Amendment Guarantee
 - Freedom of Information Acts
- Remember, the media is considered an independent "watch dog" in a free society
- Animosity and poor relations with the media will be a bigger problem for the organization than having a cooperative approach

Rules for Working with the Media

- Cooperatively provide information accorded by law
- Don't attempt to withhold information that is not positive toward the organization.
- Make certain all information provided is accurate
- Work with the media to get necessary information to the public
- Understand and work media deadlines
- View the media like an animal: "It must be fed when it is hungry because if you don't feed it, it will eat you"

Rules for Working with the Media

- Don't get mad at reporters; cooperate with them
- Have a clear understanding of each other's roles
- Don't rely on the fact that "off-the-record" comments will stay confidential
- Good relations with the media can translate to positive public perceptions
- Favorite Nations Status

Scenario

- It is approximately 10:30 a.m. on a Tuesday when you hear gunfire in your library. You look and see a man with a gun in the southwest corner of your building



General Security Practices Plan

- You and your employees remember your training on the General Security Practices Plan
- You remember the three goals of every incident: Life Safety; Incident Stabilization; Property Conservation
- Because of your pre-planning you know there is no place to securely hide so you follow your plan and pull the fire alarm so everyone evacuates the building (Life Safety)
- You call 911 (Incident Stabilization)

Incident Management Plan

- Upon exiting the building you continue to hear gunfire and see smoke coming from the building
- The police and fire departments arrive within 5 minutes



Incident Management Plan

- The police tactically enter the library and find three (5) deceased people inside
- The fire department enters and extinguishes the fire
- The fire department Battalion Chief states that the fire was intentionally set in the men's restroom
- There was significant damage to the restroom and some smoke and water damage to the children's book section

Incident Management Plan

- You reference your IMP and start the incident communication chain
- You follow your check lists in the plan for:
 - Fire
 - Death
 - Criminal Incident
- You have a prepared statement for the media

Incident Management Plan

- It is 6:30 p.m. and the police and fire departments have left. You have gone inside the library and determined that restoration needs to occur
- You communicated to the media that the library will not be open tomorrow and you will provide another update by 3:00 p.m. tomorrow



Incident Management Plan

- You made contact with your insurance agent
- You are notified by the police that it appears to be a murder - suicide
- A man shot and killed his wife and their 5 year old son, two other library patrons, started a fire in the men's restroom, then shot and killed himself



Business Continuity

- You reference your Business Continuity Plan and contact the pre-approved smoke and water restoration contractor. You also contact a general contractor for repairs to the bathroom
- You make arrangements for portable restrooms to be delivered to the site
- The contractors assist you in segregating the damaged areas

Business Continuity

- An Environmental Health contractor is brought in the next day and certifies the library is safe for occupancy
- You contact a neighboring library who agrees to loan you an allotment of children's books. As part of your plan, you remove 4 of the 10 computers in your computer lab to make space for the books

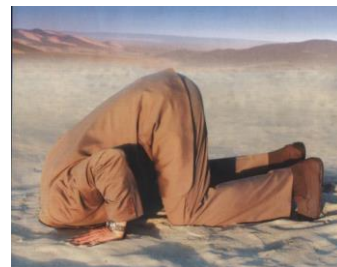
Business Continuity

- Three days from the start of the incident you are back open for business
- The restoration / re-building process takes four weeks to complete
- You are back to normal operations one month after the incident, but only closed your operation for three days



Final Thought

- "A goal without a plan is just a dream"



Questions??



Notes