# Crisis Management

**By:**
**Abdul Halim Hashim**
**Head, Occupational Safety & Health Unit**
**Lecturer, Faculty of Cognitive Sciences & Human Development**
**Universiti Malaysia Sarawak**
**hahalim@unimas.my**

# PREAMBLE

- Unplanned events can have a devastating effect on businesses.
- Crises such as fire, damage to stock, illness of key staff or IT system failure could all make it difficult or even impossible to carry out our normal day-to-day activities.
- At worst, this could see us losing customers and irreparable damage to UNIMAS reputation.
- But with good management, we can take steps to minimise the potential impact of a disaster - and ideally prevent it happening in the first place.

# Some interesting facts…

- Paraskevas (2009), 60% of organisational crises normally emit warning signals early enough to be prevented.
- 43% of companies experiencing a disaster never recover
- 40% of companies that have CM plans do not have a team dedicated to disaster recovery
- 43% of companies that have a business continuity plan do not test it annually

# Some interesting facts…

- 80% of companies have not developed CM to provide IT coverage for business continuity
- Of those who have had a crisis, 42% STILL do not have a plan!
- yet…97% felt confident that they could respond well to a crisis
- Only 23% of businesses have no early warning of some kind; about 75% of crises result from inappropriate action or inaction by top management

(UK Statistics, 2012)

# Crisis Management Vs Business Continuity Plan

- A Crisis Management Plan (CMP) and a Business Continuity Plan (BCP) are usually two different documents that can work together or separately

**You can have a crisis without a disaster**

A Crisis can exist with NO physical damage to facilities or technologies

**You can have a disaster without a crisis**

You can have a loss to physical facilities or technologies and NOT have a crisis.

**Both will escalate if not managed**

# Crisis Management Vs Business Continuity Plan

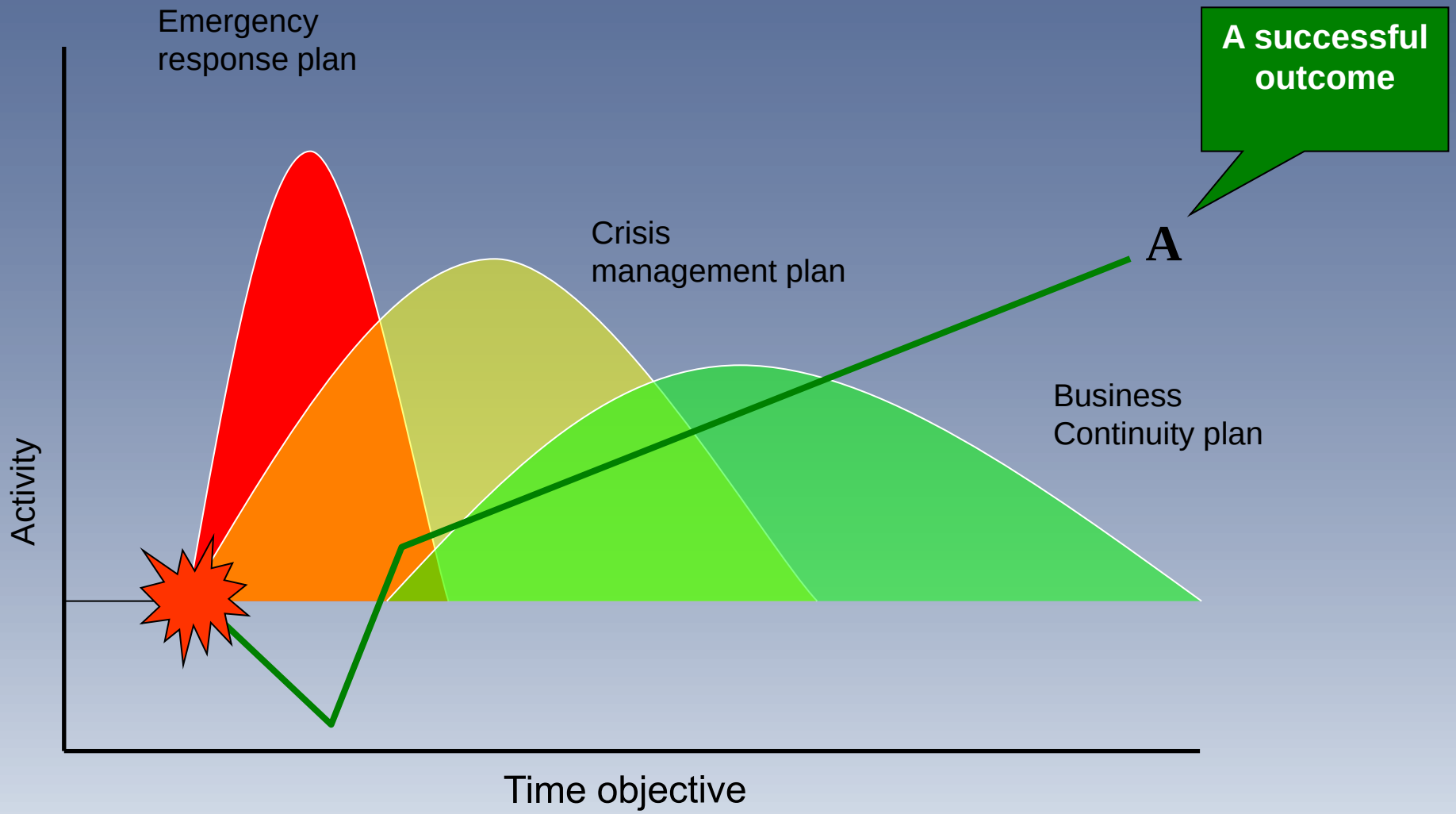
**Business Continuity Plan**

- To recover mission critical business services and processes
- Limited scenarios
- Focus on facilities and technology

**Crisis Management Plan**

- To limit intensity, manage and control negative results of an event
- Many scenarios
- Focus on people, products, services and/or reputation

# Crisis Management Vs Business Continuity Plan



# Why We Need To Plan For Possible Crises

- Failure to plan could be disastrous:
  - Damage reputation
  - Lose existing customers and the faith of potential customers
  - Lose expensive assets
  - Idle for long period of time
  - Lose money unnecessarily

# Bad News Travel Fast On Social Media

# Crises That Could Affect Our Business

- Natural disasters
  - for example, flooding caused by burst water pipes or heavy rain, or wind damage following storms.
- Theft or vandalism
  - theft of computer equipment, for instance, could prove devastating. Similarly, vandalism of machinery or vehicles could not only be costly but also pose health and safety risks.
- Fire
  - Even small fire can incapacitate a critical business function (server room for example).
- Power cut
  - loss of power could have serious consequences. What would you do if you couldn't use IT or telecoms systems or operate other key machinery or equipment?

# Crises That Could Affect Our Business

- IT system failure
  - computer viruses, attacks by hackers or system failures could affect employees' ability to work effectively.
- Restricted access to premises
  - how would your business function if you couldn't access your workplace - for example, due to a gas leak?
- Loss or illness of key staff
  - if any of your staff is central to the running of your business, consider how you would cope if they were to leave or be incapacitated by illness.
- Outbreak of disease or infection
  - an outbreak of an infectious disease among staff, or among students could present serious health and safety risks.

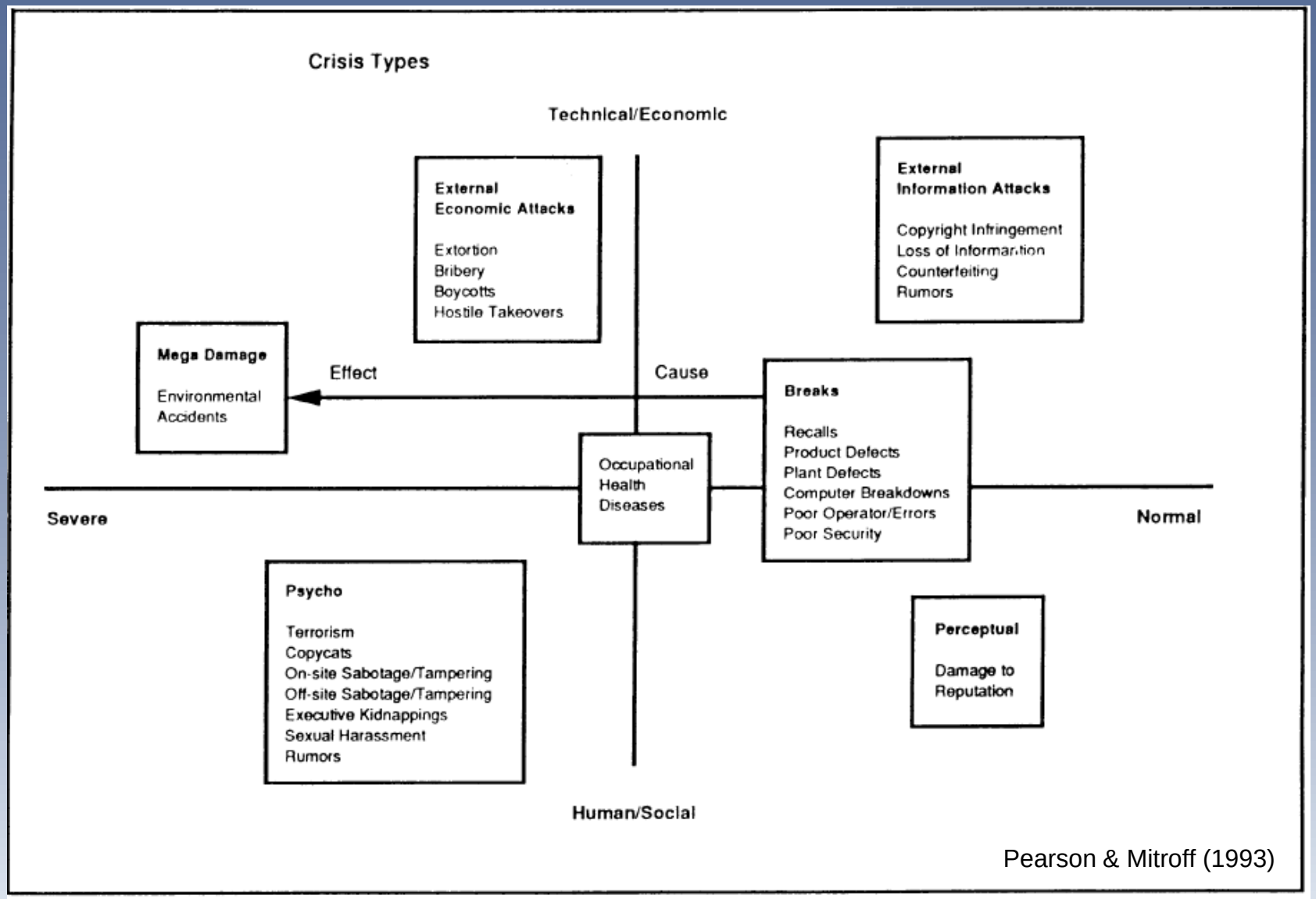
# Crises That Could Affect Our Business

- Terrorist attack
  - consider the risks to your employees and your business operations if there is a terrorist strike, either where your business is based or in locations to which you and your employees travel. Also consider whether an attack may have a longer-term effect on your particular market or sector.
- Crises affecting suppliers
  - how would you source alternative supplies?
- Crises affecting customers
  - will insurance or customer guarantees offset a client's inability to take your goods or services?
- Crises affecting your business' reputation
  - how would you cope, for example, in the event of libel in social networks?

*Though some of these scenarios may seem unlikely, it's prudent to give them consideration.


external
Terrorist/ Criminal Threat/ Incident
Activist Issue/ Protest
Structure/ Ownership Issue (e.g., hostile takeover)
Consumer Complaint/ Issue
Category/ Industry Issue
Natural Disaster
Competitor Threat
Traditional
Crisis
Triggers
Environmental Issue or Accident
Poor Financials or Stock Performance
Management Change/ Dismissal
Product Defect/ Recall
Labor Dispute
Investigation, Lawsuit, Fine, Settlement
Structure/ Ownership Issue (e.g. merger)
Incident/ Allegation of Mismanagement
Incident/ Allegation of Wrongdoing
Employee Complaint/ Issue
Workplace Injury/ Fatality
internal
social@Ogilvy

# Crisis Typology




Pearson & Mitroff (1993)

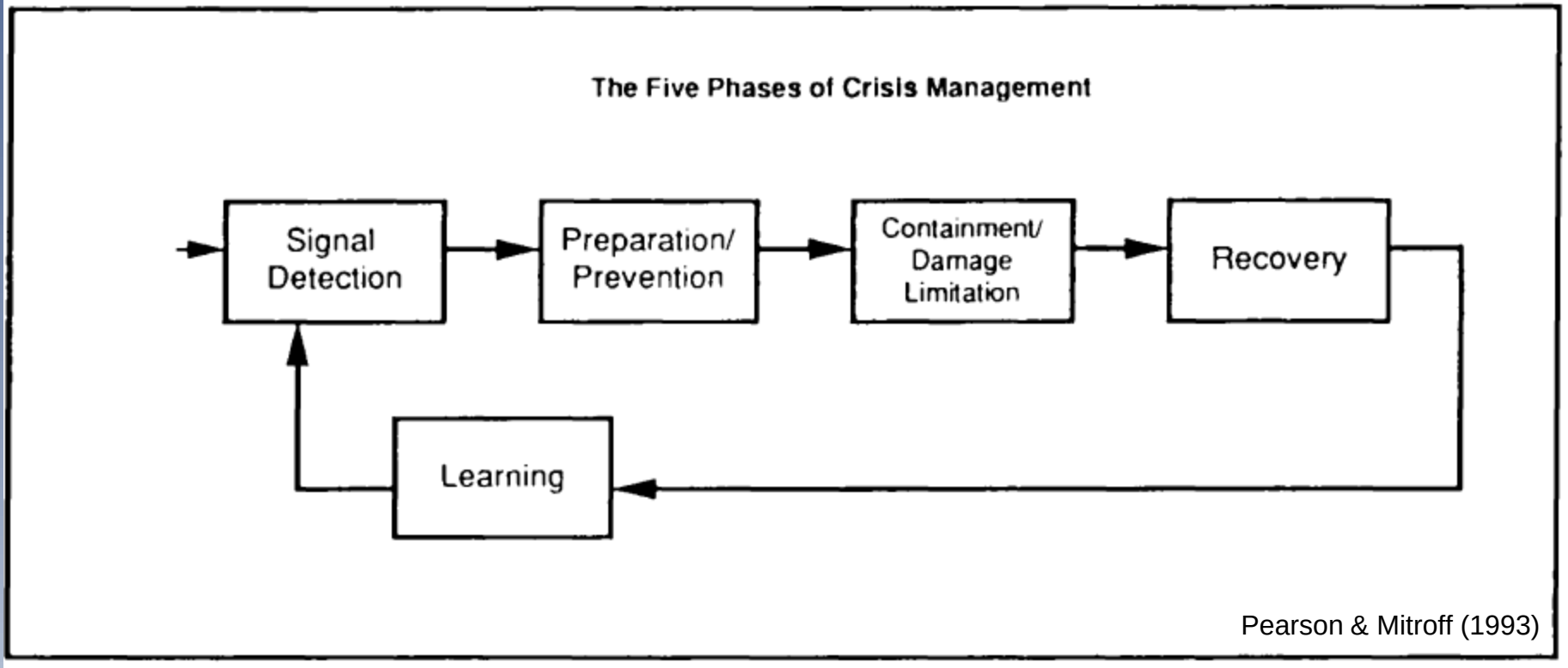
# Crisis Typology

- Crisis preparation begins with an understanding of the nature of a specific type of crisis.
- In-depth knowledge on how to deal with each of the six types of crises can strengthen an organization's ability to manage other crises within the same type.
- Organizational learning in preparation for one specific crisis is transferable to other crises within the same type. Decision making and action plans are similar within each type.
- Organizations should prepare for at least one potential crisis in each of the seven types to confer the broadest range of crisis preparation with minimal investment.

# Crisis Typology

- In every crisis situation, no single crisis has occurred in isolation.
- The simultaneous occurrence of multiple crises has been the norm.
- A mismanaged crisis (of a single type) can set off a chain reaction of other crises.
- Thus, in principle, every type is capable of being the "cause" or the "effect" of every other.
- It is recommended that organizations plan for the simultaneous occurrence of multiple crises.

# The Five Phases Of Crisis Management




**Organization can increase their ability to manage crises by properly managing each phase of the process**

# Phase 1: Signal Detection

- Crises leave a trail of early warning signals.
- In many cases, organizations not only ignore such signals, but may actually exert considerable efforts to block them.
- Organizations which prepare effectively for crises constantly probe and scrutinize their operations and management structures for potential errors or problems before they are too big to correct.
- They establish clear and open information channels and recognize the contributions of messengers of bad news.

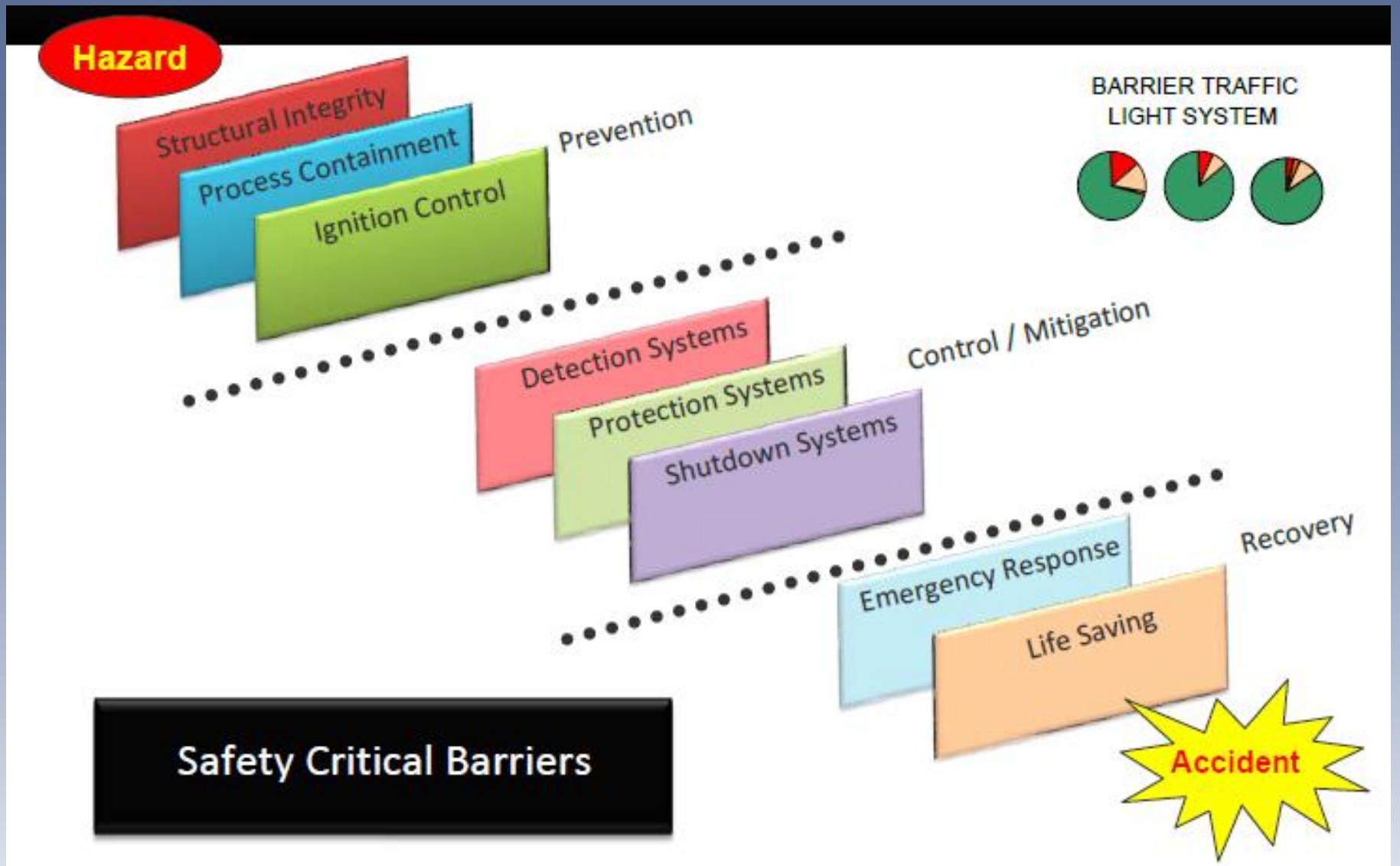
# Signal Not Detected: Bhopal Tragedy 1984

- As Bisarya and Swaraj (Mayor and Police Chief's of Bhopal at that time) explained, Bhopal tragedy happened mainly because of two facts. In first place, safety systems failed or were inoperable and secondly, safety procedures were not complied.
- Prior to the tragedy, in 1981 and 1982, three accidents already occurred:
  1. December 1981: One worker died while handling phosgene
  2. February 1982: 25 workers were hospitalized because of chlorine, MIC and hydrochloric acid's leaking
  3. December 1982: Massive leak of chlorine workers and neighbors were affected

After these accidents, the Legislative Assembly of the State concluded that "there was no danger to Bhopal nor will there ever be!" (Bisarya and Swaraj, 2005).

# Phase 2: Preparation/Prevention

- creation of crisis teams
- Policy and procedures etc.
- crisis training and simulation exercises.


Hazard
Structural Integrity
Process Containment
Ignition Control
Prevention
BARRIER TRAFFIC LIGHT SYSTEM
Detection Systems
Protection Systems
Shutdown Systems
Control / Mitigation
Emergency Response
Life Saving
Recovery
Accident
Safety Critical Barriers

# Phase 3: Containment / Damage Limitation

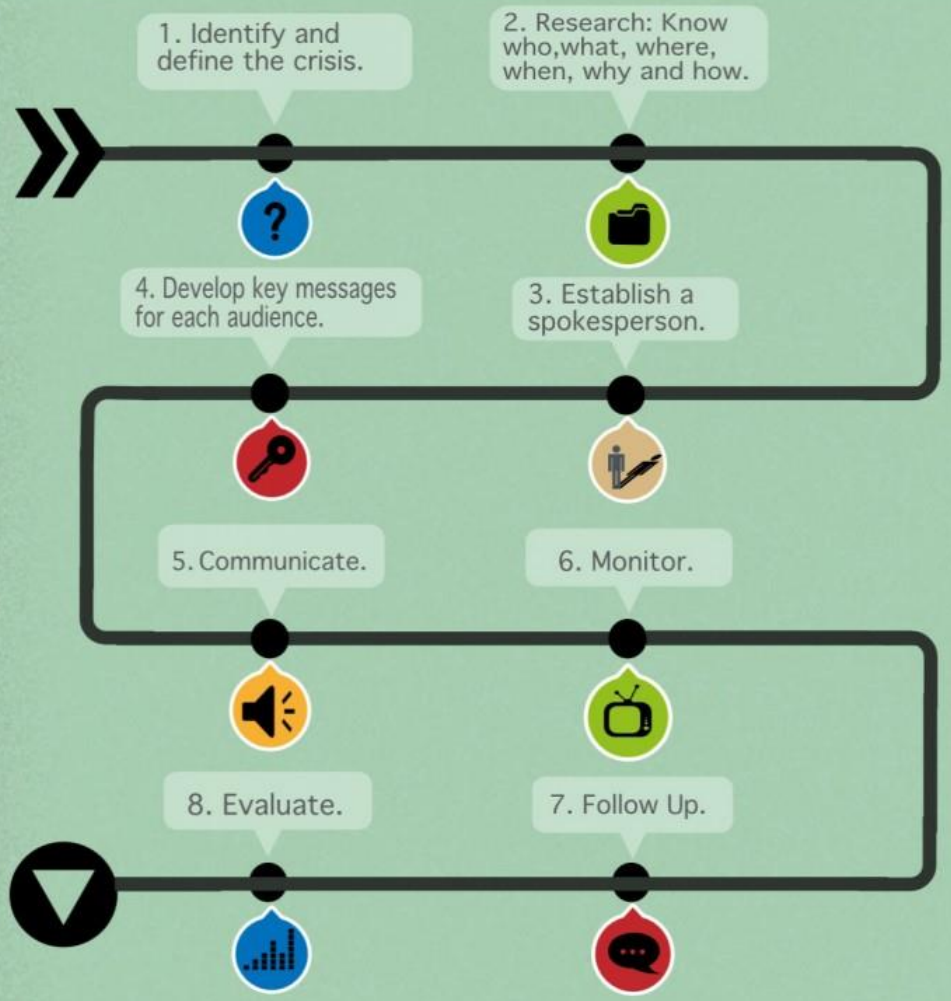
- The intent of the third phase, damage containment, is to limit the effects.
- Detail plans for preventing a localized crisis from affecting other uncontaminated parts of the organization or its environment.
- Some examples:
  - Evacuation and escape
  - Spill containment
  - Fire protection systems (sprinkler, water deluge, CO)
  - Temporary refuge
  - Recall defective product
  - Public relations event

# Crisis Communications

- Good communication is the heart of any crisis management plan
- To reduce tension, demonstrate a corporate commitment to correct the problem and take control of the information flow.
- Involves communicating with a variety of stakeholders: the media, employees, neighbors, investors, regulators and lawmakers.
- Public relations is the single most important element of the crisis response.
- Create guidelines for designated spokesperson covering how working with the media and community leaders.
- Prepare templates for communicating with various scenarios.
- Attorneys on the crisis management team should review media statements and proposed answers.

# Communicating During A Crisis

Tell the truth. Tell it quickly. Tell it often.




While every crisis situation is different and requires a unique and tailored approach, it is essential to have a plan in place to ensure strategies are implemented in a timely and effective manner.

# Phase 4: Recovery

# Phase 5: Learning

- Refers to adequate reflection and critical examination of the lessons learned from experiencing a crisis.

- Well-prepared organizations examine the factors that enabled them to perform well, versus those that inhibited their performance.

# Crisis Capabilities

The depth of preparation will depend on:

- Technical
  - Safe and reliable machines, equipment and tool
  - Reliable emergency systems – alarms, shutdown etc.

- Human factor
  - Human-machine interactions

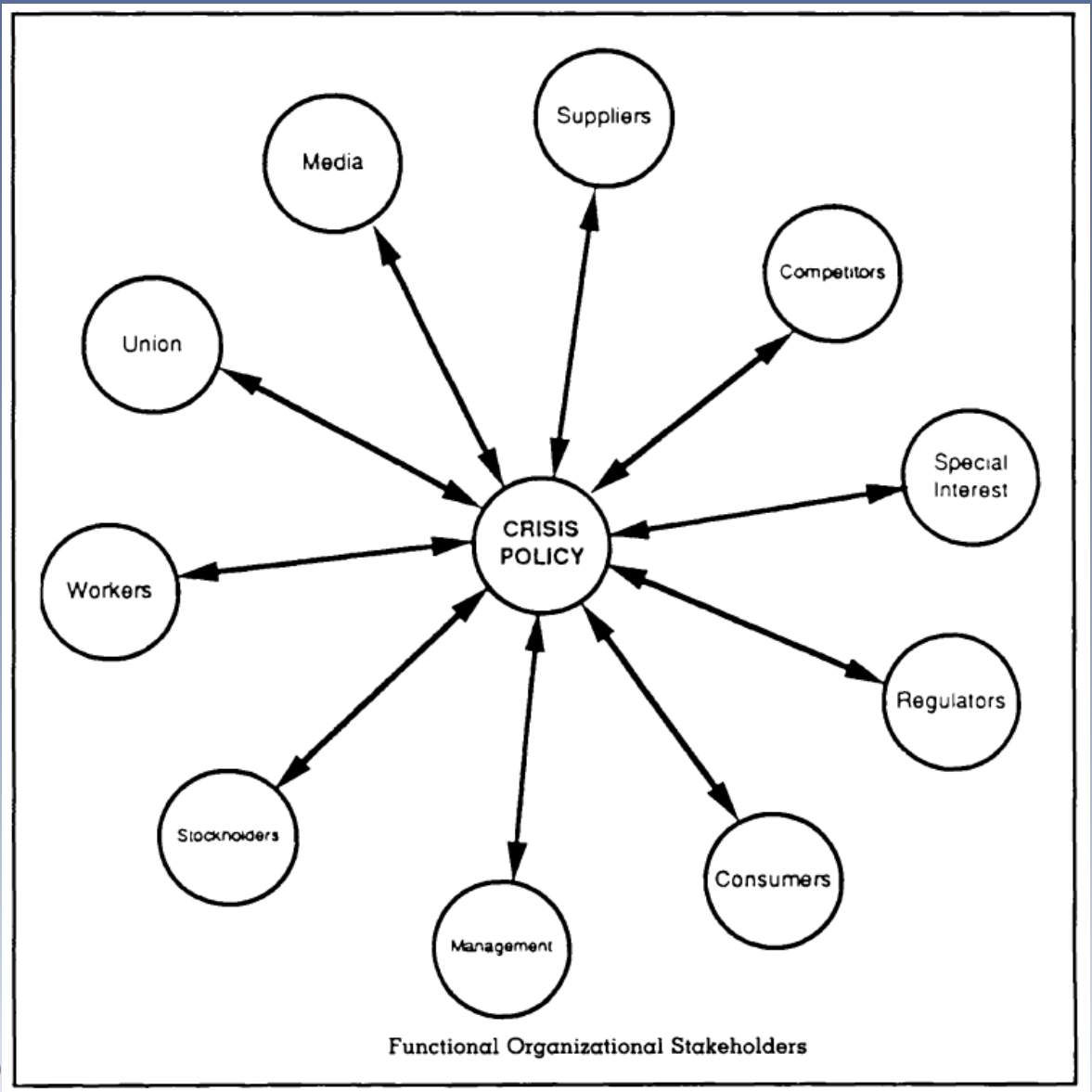
- Infrastructural
  - Open and effective communication channels among levels and across divisions
  - Accountability
  - Crisis management teams

# Crisis Capabilities

The depth of preparation will depend on:

- Cultural & Belief
  - Does cultural systems support or impede CM efforts?
  - Ultimately, senior executives' attitudes and beliefs regarding the organization's potential for crises, and the organization's ability to prepare for and manage crises will determine the success of crisis management.

# Stakeholders




Functional Organizational Stakeholders

Pearson & Mitroff (1993)

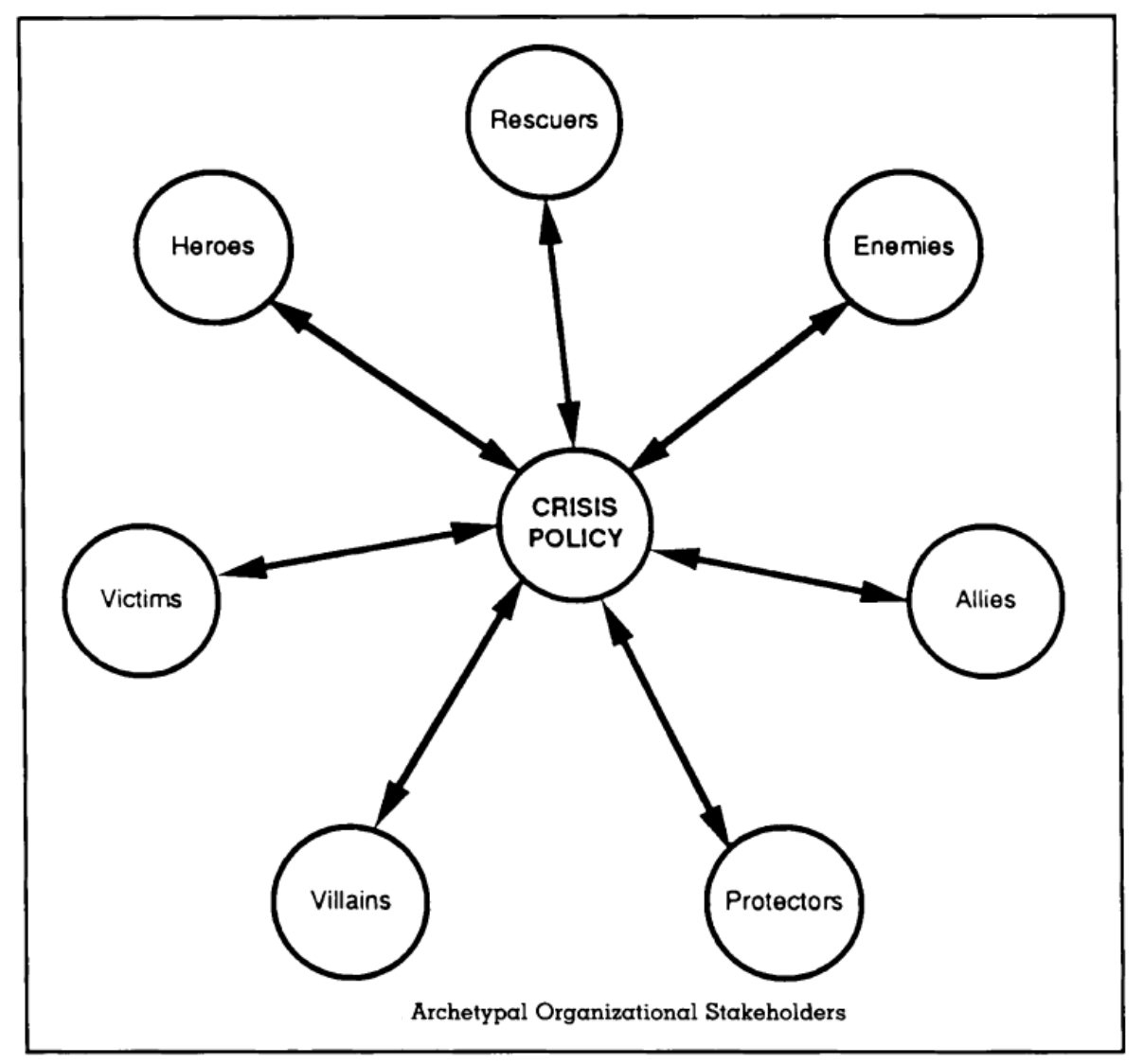
# Stakeholders

- Organizations must recognize that a crisis has the potential to affect not only themselves and their products, but also potential stakeholders: consumers, competitors, suppliers, and members of their general environment.

- Many have made positive assumptions about their key stakeholders (e.g., as "allies," "rescuers") only to find that under crisis conditions their assumptions were faulty.

- In some cases, allies and rescuers have abandoned the stricken organization to protect their own interests by distancing themselves from the crisis.

# Stakeholders



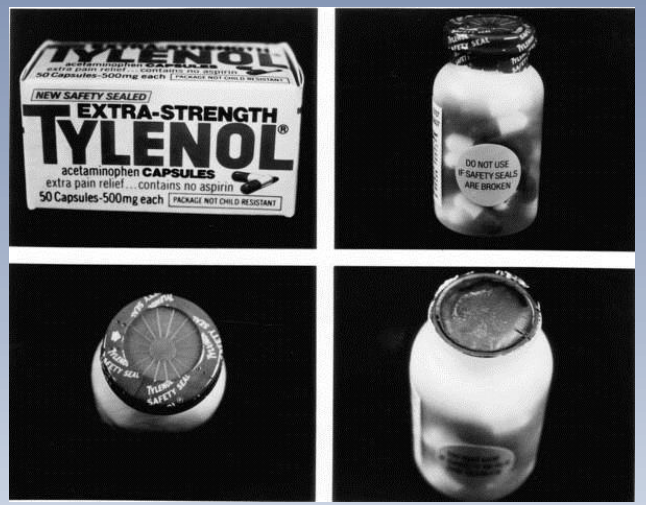
Archetypal Organizational Stakeholders

Pearson & Mitroff (1993)

# Examples Of Successful Crisis Management

**Tylenol (Johnson and Johnson)**

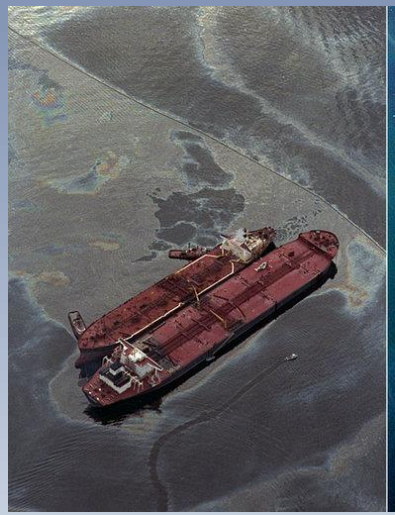
- In the fall of 1982, a murderer added 65 milligrams of cyanide to some Tylenol capsules on store shelves, killing 7 people, including 3 in one family.
- Johnson & Johnson recalled and destroyed 31 million capsules at a cost of $100 million.
- The CEO appeared in television ads and at news conferences informing consumers of the company's actions.
- Tamper-resistant packaging was rapidly introduced, and Tylenol sales swiftly bounced back to near pre-crisis levels.
- When another bottle of tainted Tylenol was discovered in a store, it took only a matter of minutes for the manufacturer to issue a nationwide warning that people should not use the medication in its capsule form.

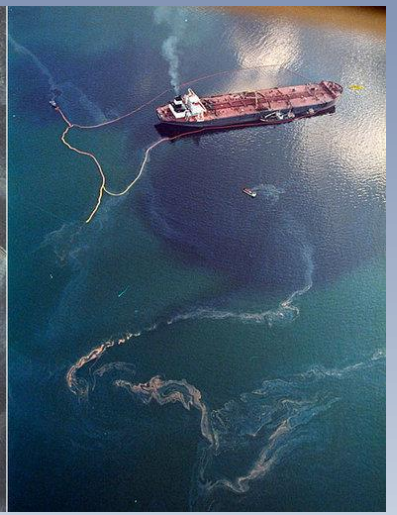



# Examples Of Unsuccessful Crisis Management

Exxon

- On March 24, 1989, a tanker belonging to the Exxon Corporation ran aground in the Prince William Sound in Alaska.
- The Exxon Valdez spilled millions of gallons of crude oil into the waters off Valdez, killing thousands of fish, fowl, and sea otters.
- Hundreds of miles of coastline were polluted and salmon spawning runs disrupted; numerous fishermen, especially Native Americans, lost their livelihoods.





# Examples Of Unsuccessful Crisis Management

- What happened?
  - Exxon did not react quickly in terms of dealing with the media and the public
  - the CEO did not become an active part of PR effort and actually shunned public involvement
  - Exxon did not have a communication plan or a communication team to handle the event—in fact, the company did not appoint a PR manager to its management team until 1993, 4 years after the incident
  - Exxon established its media center in Valdez, a location too small and too remote to handle the onslaught of media attention
  - the company acted defensively in its response to its publics, even laying blame, at times, on other groups such as the Coast Guard.

# BUSINESS CONTINUITY PLAN

# BUSINESS CONTINUITY PLAN

Benefits of a business continuity plan (BCP)

- BCP will make coping in a crisis easier and enable us to minimise disruption to the business and its customers.

- Prove to customers, insurers and investors that our business is robust enough to cope with anything that might be thrown at us - possibly giving us the edge over our competitors

# BUSINESS CONTINUITY PLAN

A BCP typically includes five sections:

1. BCP Governance
2. Business Impact Analysis
3. Plans, measures and arrangements for business continuity
4. Readiness procedures
5. Quality assurance technique (exercise, maintenance and auditing)

# BCP GOVERNANCE


Leadership framework for crisis management

# BCP Central Committee

BCP Committee would normally:

- approve the governance structure;
- clarify their roles, and those of participants in the program;
- oversee the creation of a list of appropriate committees, working groups and teams to develop and execute the plan;
- provide strategic direction and communicate essential messages;
- approve the results of the BIA;
- review the critical services and products that have been identified;
- approve the continuity plans and arrangement;
- monitor quality assurance activities; and
- resolve conflicting interests and priorities.

# Business Impact Analysis (BIA)

- Quantifies loss due to business outage (financial, extra cost of recovery, embarrassment)
- Does not estimate the probability of kinds of incidents, only quantifies the consequences

A BIA typically includes five sections

- identify the organization's mandate and critical services or products
- rank the order of priority of services or products for continuous delivery or rapid recovery
- identify internal and external impacts of disruptions.

# Business Impact Analysis (BIA)

1. **Identify the mandate and critical aspects of an organization**

   - This step determines what goods or services it must be delivered.

   - Information can be obtained from the mission statement of the organization, and legal requirements for delivering specific services and products.

# Business Impact Analysis (BIA)

**Prioritize critical services or products**

- Based on minimum acceptable delivery levels and the maximum period of time the service can be down before severe damage to the organization results.

- To determine the ranking of critical services, information is required to determine impact of a disruption to service delivery, loss of revenue, additional expenses and intangible losses.

# Business Impact Analysis (BIA)

**Identify impacts of disruptions**

- how long UNIMAS could function without the service or product, and how long clients would accept its unavailability.
- necessary to determine the time period that a service or product could be unavailable before severe impact is felt.
- Other terms would include ‘Maximum Tolerable Downtime (MTD)’ or ‘Maximum Allowable Outage (MAO)’

# Business Impact Analysis (BIA)

**Identify impacts of disruptions**

- A good question would be “what would be the loss to the business if we suffered the total loss of our data center?”

- Some losses may be quantified fairly exactly.

- Others have to be estimated as carefully as possible. An example would be the cost to the business in loss of consumer confidence from an extended outage.
  - For instance, what if UNIMAS were unable to hold classes for four weeks because we couldn’t deliver our electronic instruction? How would parents of UNIMAS students react to that? And how much would it cost?

# Business Impact Analysis (BIA)

**Identify areas of potential revenue loss**

- To determine the loss of revenue, it is necessary to determine which processes and functions that support service or product delivery are involved with the creation of revenue.

- If these processes and functions are not performed, is revenue lost? How much?
- If services or goods cannot be provided, would the organization lose revenue?
- If so, how much revenue, and for what length of time?
- If clients cannot access certain services or products would they then to go to another provider, resulting in further loss of revenue?

# Business Impact Analysis (BIA)

**Identify additional expenses**

- If a business function or process is inoperable, how long would it take before additional expenses would start to add up?
- How long could the function be unavailable before extra personnel would have to be hired?
- Would fines or penalties from breaches of legal responsibilities, agreements, or governmental regulations be an issue, and if so, what are the penalties?

# Business Impact Analysis (BIA)

**Identify intangible losses**

- Estimates are required to determine the approximate cost of the loss of consumer and investor confidence, damage to reputation, loss of competitiveness, reduced market share, and violation of laws and regulations.

- Loss of image or reputation is especially important for public institutions as they are often perceived as having higher standards.

# Business Impact Analysis (BIA)

**Insurance requirements**

- If we can’t afford to pay the full costs of a recovery; having insurance ensures that recovery is fully or partially financed.

- When considering insurance options, decide what threats to cover.
  - Use the BIA to help decide both what needs insurance coverage, and the corresponding level of coverage.
  - Some aspects of an operation may be overinsured, or underinsured.
  - Minimize the possibility of overlooking a scenario, and to ensure coverage for all eventualities.

- Document the level of coverage and examine the policy for uninsured areas and non specified levels of coverage.

# Business Impact Analysis (BIA)

**Insurance requirements**

- Property insurance may not cover all perils (steam explosion, water damage etc.). Coverage for such eventualities is available as an extension in the policy.

- Include an expert or an insurance team when developing the response plan.

# Business Impact Analysis (BIA)

**Ranking**

- Once all relevant information has been collected and assembled, rankings for the critical business services or products can be produced.
- Ranking is based on the potential loss of revenue, time of recovery and severity of impact a disruption would cause.
- Minimum service levels and maximum allowable downtimes are then determined.

# Business Impact Analysis (BIA)

**Identify dependencies**

- Identify the internal and external dependencies of critical services or products

- Internal dependencies include
  - employee availability
  - equipment, facilities, computer applications, data, tools, vehicles
  - support services such as finance, human resources, security and information technology support.

# Business Impact Analysis (BIA)

**Identify dependencies**

- External dependencies include
  - suppliers
  - external corporate assets such as equipment, facilities, computer applications, data, tools, vehicles
  - external support services such as facility management, utilities, communications, transportation, finance institutions, insurance providers, government services, legal services, and health and safety service.

# Plans For Business Continuity

- Detail the ways and means to ensure critical services and products are delivered at a minimum service levels (identified in BIA) within tolerable down times.

- Continuity plans should be made for each critical service or product.

# Plans For Business Continuity

**Mitigating threats and risks**

- Threats and risks are identified in the BIA or in a full-threat-and-risk assessment.
- Identify risk control measures or mitigation plan
- For example, if an organization requires electricity for production, the risk of a short term power outage can be mitigated by installing stand-by generators.
- Another example: if an organization that relies on telecommunications to function effectively, failures can be minimized by using alternate communications networks, or installing redundant systems.

# Plans For Business Continuity

**Analyze current recovery capabilities**

- Consider recovery arrangements the organization already has in place, and their continued applicability.

- Include them in the BCP if they are relevant.

- For example:
  - existing data back-up plan
  - emergency stand-by generators in building

# Plans For Business Continuity

- Ensure that plans are made for increasing levels of severity of impact from a disruption.
  - For example, if limited flooding occurs beside an organization's building, sand bagging may be used in response.
  - If water rises to the first floor, work could be moved to another company building or higher in the same building.
  - If the flooding is severe, the relocation of critical parts of the business to another area until flooding subsides may be the best option.
- Another example:
  - the uses paper forms to keep track of inventory until computers or servers are repaired, or electrical service is restored.
  - For large financial firms, any computer disruptions may be unacceptable, and an alternate site and data replication technology must be used.

# Plans For Business Continuity

- Proper response requires teams to lead and support recovery and response operations.
- Team members should be selected from trained and experienced personnel who are knowledgeable about their responsibilities.

# Plans For Business Continuity

**Response preparation**

- The number and scope of teams will vary depending on organization's size, function and structure, and can include:
  - Command and Control Teams that include
    - a Crisis Management Team, and
    - a Response, Continuation or Recovery Management Team.

# Plans For Business Continuity

Task Oriented Teams that include

- an Alternate Site Coordination Team
- Contracting and Procurement Team
- Damage Assessment and Salvage Team
- Finance and Accounting Team
- Hazardous Materials Team
- Insurance Team
- Legal Issues Team
- Telecommunications/ Alternate Communications Team
- Mechanical Equipment Team
- Mainframe/ Midrange Team
- Notification Team
- Personal Computer/ Local area Network Team
- Public and Media Relations Team
- Transport Coordination Team
- Vital Records Management Team

# Plans For Business Continuity

**Alternate facilities**

- If an organization's main facility or IT assets, networks and applications are lost, an alternate facility should be available.

- There are three types of alternate facility: Cold site, Warm site and Hot site

  - Cold site
    - not furnished and not equipped for operation.
    - Proper equipment and furnishings must be installed before operations can begin
    - substantial time and effort is required to make a cold site fully operational.
    - the least expensive option

# Plans For Business Continuity

**Alternate facilities**

- Warm site
  - electronically prepared and almost completely equipped and furnished for operation.
  - can be fully operational within several hours.
  - more expensive than cold sites.

- Hot site
  - fully equipped, furnished, and often even fully staffed.
  - can be activated within minutes or seconds.
  - the most expensive option.

# Plans For Business Continuity

**Alternate facilities**

- Mutual aid agreements with other similar organization (say for example UiTM?)
  - I'll help you if you'll help me!
  - Inexpensive
  - Usually not practical

# Readiness Procedures

**Training**

- All employees and staff briefed on the contents of the BCP and aware of their individual responsibilities
- Having employees with direct responsibilities trained for tasks they will be required to perform, and be aware of other teams' functions

# Readiness Procedures

**Exercises/Drill**

- To achieve and maintain high levels of competence and readiness.
- While exercises are time and resource consuming, they are the best method for validating a plan.
- A plan that is not validated is not actually a good plan

# Quality Assurance Techniques

- Objective: To assess the plan's accuracy, relevance and effectiveness.
- It should also uncover which aspects of a BCP need improvement.
- The appraisal can be performed by an internal review, or by an external audit.

# BCP Case: Ericsson vs. Nokia

# BCP Additional Source Of Reference

- Harvard University
  - http://www.ehs.harvard.edu/programs/business-continuity
- University of Aberdeen
  - http://www.abdn.ac.uk/staffnet/governance/business-continuity-352.php
- Indiana University
  - http://protect.iu.edu/emergency/bcp

# THANK YOU