BUSINESS CONTINGENCY PLANNING
March 2003

Assessing Business Risk and Impact of Potential Emergencies

To begin the Business Contingency Planning (BCP) Process you should complete the assessment of the potential risks to the business, which could result from disasters or emergency situations, outlined below. It is necessary for you to consider all the possible incidents and the impact each may have on the organization's ability to continue to deliver its normal business services. You should consider organizing a BCP Project Team to get various viewpoints and perspectives.

1. Emergency Incident Assessment

A key part of the BCP development process is for you to review the types of disruptive events that can affect the normal business process. We have included a broad range (numbers 1 - 7) of possible scenarios for your consideration.

Each one of the scenarios itemized below should be examined thoroughly and should be rated for possibility of occurrence (probability rating), and level of impact (impact rating).

Probability Rating	
Score	*Level*
5	Very High
4	High
3	Medium
2	Low
1	Very Low

Impact Rating	
Score	*Level*
5	Catastrophic
4	Devastating
3	Critical
2	Controllable
1	Irritating

As a general rule: anything with a score > 10 when multiplied against each other requires a contingency plan with specific actions to minimize risks.

A. Environmental Disasters

Tornado	Electrical Storms
Hurricane	Fire
Flood	Heat
Snowstorm	Freezing Conditions

Drought
Earthquake
Epidemic

B. Organized and / or Deliberate Disruption

Your BCP Project Team will need to examine each potential disaster or emergency situation caused through activities which can be described as "organized disruption". The focus should be on the level of business disruption likely from each situation.

Act of Terrorism
Acts of terrorism include explosions, bomb threats, hostage taking, sabotage and organized violence.

Act of Sabotage
An act of sabotage is the deliberate serious disruption of an organization's activities with an attempt to discredit or financially damage the organization.

Act of War / Mobilizing of Troops
Call to arms – reservists, active duty. Priority of US Government Contract.

Theft
This hazard could range from the theft of goods or equipment to the theft of money or other valuables.

Arson
Arson is the deliberate setting of a fire to damage the organization's premises and contents.

Labor Disputes / Industrial Action
This disruptive threat is the withdrawal of labor or working to rule usually organized by a union to which employee groups may belong. Verify supply chain labor contracts, dates, impact, etc.

C. Loss of Utilities and Services

The focus here should be on the level of business disruption likely from each loss of utilities or public services.

Electrical power failure
All organizations should be prepared for a possible electrical power failure, as the impact can be so severe. Data can be lost, customer's information can be lost and there can be a serious impact on revenue.

Loss of gas supply

The loss of gas supply can be extremely serious where the business relies on gas to fuel its production processes or provide heating. The impact that a loss of gas supply can have can result in the whole process shutting down.

Loss of water supply

Petroleum and Oil Shortage

Communications Services Breakdown

A disruption to the telecommunications services can result in a business losing revenue and customers.

D. Equipment or System Failure

Internal Power Failure

Heating/Air conditioning Failure

An air conditioning (AC) failure could have serious consequences where the AC unit is protecting particularly sensitive equipment.

Production Line / Equipment Failure

Mechanical or electronic failure on an organization's production line particularly vulnerable is the fully automated processes.

Cooling Plant Failure

E. IT and Communications Failure

Types of threats to computer systems are many and varied, including hardware failure, damage to cables, water leaks and fires, air conditioning system failures, network failures, application system failures, telecommunications equipment failures etc.

Specifications of IT and Communication Systems and Business Dependencies

The BCP should contain a detailed specification of the main IT business processing systems and network configurations.
This list should include the key business processes that are dependent upon each critical system component.

Key IT, Communications and Information Processing Systems

List the most critical IT processes and information processing systems to identify which business processes will be affected when there is an interruption to the IT system availability. Developing a back-up and recovery strategy.

Key IT Personnel and Emergency Contact Information

Lists of key IT personnel and their emergency contact information. The persons responsible for back up and recovery of specific systems can be contacted in the event of a significant unexpected event which is affecting the IT systems and is likely to disrupt normal business operations.

- Key Contact Personnel
- Normal Contact Name
- Emergency Contact

Key IT and Communications Suppliers and Maintenance Engineers

A list of key IT and communications suppliers and contracted maintenance engineers should be prepared and maintained, together with emergency contact information.

Existing IT Recovery Procedures

A summary of the existing IT back up and recovery procedures should be documented within the BCP. This information should cover both hardware and software systems in addition to data back up and recovery processes. Information should also be included on any off-site data storage.

F. Serious Information Security Incidents

Cyber Crime

Cyber crime is a major area of information security risk. IT includes attacks by hackers, denial of service attacks, virus attacks, hoax virus warnings and premeditated internal attacks.

Loss of Records or Data

The loss of records or data can be particularly disruptive where poor back up and recovery procedures result in the need to a re-input and re-compile the records. This is normally a slow process and is particularly labor intensive.

Disclosure of Sensitive Information

Types of serious disclosure involve secret patent information, plans and strategic directions, secret recipes or ingredients, information disclosed to legal representatives etc.

G. Other Emergency Situations

Workplace Violence

Neighborhood Hazard

An example would be seepage of hazardous waste from a neighboring factory or the escape of toxic gases from a local chemical plant. Health and safety regulations require that the organization take suitable action to protect its employees.

Health and Safety Regulations / OSHA Requirements

For organizations that do not properly and fully observe all the necessary Health and Safety Regulations, a complaint or an inspection can result in the operation being completely closed down until the situation is corrected.

Legal Problems

Organizations can experience a wide range of legal issues including sexual harassment, contract disputes, copyright disputes, health and safety regulations and discrimination.