3-DO Telecommunications

www.3-do.net

BUSINESS CONTINUITY PLANNING (BCP)

What comes first the chicken or the egg? What comes first in contingency planning? Recovering lost technology or keeping the business running?

Contingency Planning and the Disaster Life Cycle

Given today's increased technology and necessity of network communications, Internet connectivity and expanding networks of electronic communication and specialized business processes, contingency planning for disasters is a rising priority on the agenda at executive boardroom meetings. Business continuity planning is a process that identifies the most critical functions of an organization. A business continuity plan involves the long-range considerations of an organization's business survival. A professionally structured plan covers business disruption issues like loss of telephone communications, loss of computer processing capability, and loss of accessibility to vital critical facilities. The most common mistake made in the development of a contingency plan is that the developed plan focuses on computer disasters and ignores the potential of other physical or natural disasters like fires, explosions and employee sabotage, that can render inaccessibility or critical operations inoperable.

Responsibility for business contingency plan development and auditing usually resides with the risk manager or the chief financial officer. However, more increasingly, Security Managers and Security Management Consultants have taken a more active role in plan development. The security professional experience in the protection of assets, involvement in the identification of vulnerabilities and threats and the mitigation of risk, makes them logical choices for the role.

The real threat to business continuity is in the loss of vital buildings, critical production or distribution operations resulting from natural causes or environmental conditions. Management needs to understand the different phases of an actual disaster, known as the "disaster life cycle". The disaster life cycle is a unification of the following events: prevention and preparedness, response and damage containment, protection of cash flow and restoration of facilities. The life cycle produces three required deliverables to the overall plan, which will be discussed below in detail. They include a risk management program, emergency response plan and business continuity strategies. A neutral facilitator should conduct the development and project management with input from departmental managers and not by someone from the information technology systems' staff. The detailed step- by-step specifications and procedures required to back

up and restore computer data is only part of the necessary steps needed to ensure business continuity in all operating departments.

Development of a Risk Management Program

Departmental managers should understand the part a risk management program plays in the overall business continuity plan. The risk management program is a combination of policy, objectives, procedures and physical safeguards which, when measured, reduce the impact and likelihood of a loss or disaster. A risk management program is procedural in format because its purpose is to document ongoing corporate responsibilities in each department.

Hopefully the risk management program is the only part of the overall plan that will ever be used. Without an incident or disaster there will never be a formal requirement to actually implement an emergency response exercise to an emergency, nor will there be a need to call business continuity strategies into service. A professionally prepared risk management program is of great significance because it consists of ongoing activities to help prevent the likelihood of a disaster. The implementation of such things as sound security administrative and physical safeguards measures are used to deter, deny, delay and minimize impact of a threat becoming an actual loss or disaster. Examples of this are the storage of duplicate computer records off-site so that they can be recovered and the development and training of a fire prevention brigade.

Development of an Emergency Response Plan

The organization needs to be prepared to respond to a disaster or to an emergency once it occurs. The emergency response plan usually covers the first 24 to 48 hours following a disaster. The objective of the plan is to protect and secure the health and safety of the property, personnel and information. The plan's purpose is to notify employees, assess damage, re-route incoming phone calls and or/ messages, initiate the restoration of computer-processing capability, provide medical emergency response and security to personnel. Once the emergency is stabilized, the resumption, recovery and restoration will begin. Response planning is not resumption or recovery planning but the three plans should be intertwined so there will be a smooth transition from response to recovery. Resumption embraces the initial short-term strategies and steps to get back into business as quickly as possible (e.g. hot or cold site and mutual aid operational agreements). Recovery and restoration embraces long-term strategic plans (e.g. replacement of production lines or construction of a new facility).

Business Continuity Strategies

Business continuity strategies are crucial to the overall plan. "What if" strategies for maintaining business continuity, after a disaster, should be cultivated through highly structured constructive discussion with department managers. If continuity strategies are not developed with the right mindset, and assumptions are not facilitated by an individual experienced in basic business and synergistic problem solving, they will be part of the problem instead of part of the solution. The plan must identify all critical business functions of the company with cost effective strategies to recover and resume

operations. The executive managers first duty of business is to survive, and the guiding principal of business and economics is not the maximization of profit but the avoidance of losses. The executive management objective, in the event of a physical disaster, is to do whatever is necessary to service customers, retain market share, and maintain cash flow until normal operations can be resumed. It is the planning process itself that brings true value to the overall plan if a disaster is realized.

Planning Requirements

Senior management of public corporations have a legal responsibility to their stockholders, customers, suppliers and employees to provide a contingency plan so that business functions will continue after a disaster. The Foreign Corrupt Practices Act (PL100-235), probably more than anything else, increased awareness of the lack of contingency planning in corporate America. The Foreign Corrupt Practices Act points out the fact that computerized management information systems contribute to the decision-making process and to management's control of operations, and as such, represent the life line of the organization. It also dictates that management planning related to the continued availability of these decision making systems has, for directors and high-level officers, an impact on the standards of care. These standards of duty of care would be applied to determine potential liability if, for example, lack of a contingency plan resulted in avoidable losses. Therefore, management can be held liable for inadequate planning. Some regulatory authorities that require business continuity plans in Canada and the United States of America are promulgated by:

1. Canada Labour Code
2. Federal Trade Commission
3. Chief National Bank Examiner, Banking Regulations (BC-177)
4. Office of Budget and Management
5. Health Insurance Portability & Accountability Act HIPAA (1996)

Hot Buttons

1. Is your organization prepared for a sudden disaster?
2. Of five businesses experiencing a disaster or extended outage two never reopen their doors, of the three that remain, one will close within two years.
3. It makes good business sense to have business continuity strategies, as a point of reference, should a disaster actually happen.
4. The objective of the plan is to protect your present market share, cash flow and your ability to service customers after a disaster by:

    i. Reducing the likelihood of a disaster
    ii. Responding to the disaster systematically
    iii. Ensuring business continuity during and after a disaster

    Deliverables:

    iv. Who will execute recovery options
    v. What is needed to recover, resume, continue or restore business functions

vi. Where to go to resume corporate, business and operational functions
vii. When business functions and operations must resume
viii. How procedures for recovery, resumption, continuity, and restoration will be implemented

5. A sound, professionally developed, contingency plan may reduce insurance premiums by 5% to 10% percent.

Benefits

Risk assessments provide your company with information upon which to base decisions. The ultimate goal of the risk assessment is to strike an economic balance between the impact of the risk and the cost of implementing protective measures to reduce, eliminate or transfer the risk.

3-DO Telecommunications LLC has helped numerous organizations reduce their liabilities and guard against future crises. Below are some of the areas in which we have extensive expertise:

PHYSICAL SECURITY

- Security policy and procedures
- Fully networked C.C.T.V. surveillance
- Electronic access control system integration

NETWORK AND DATA SECURITY

- Cybercrime issues
- Risk management and analysis
- Telecommunications network security
- Legal issues and investigations

POLICY AND PROCEDURE REVIEW

- Standard analysis
- Policy audit
- Development and implementation

BUSINESS CONTINUATION AND DISASTER RECOVERY PLANNING

- Business impact analysis
- Contingency planning
- Business continuity planning
- Emergency preparedness