BPIR.com

Business Performance
Improvement Resource

BPIR Management Brief : Vol 3 Issue 6 – Business Continuity Planning (BCP)

Author: Neil Crawford
Research assistance: Kevin McKenna
BPIR.com Ltd, Centre for Organisational Excellence Research

Welcome to Vol 3 Issue 6 of the BPIR.com Management Brief that provides short, easily digestible research summaries based on specific topics or tools. Summaries include comments from experts, case examples, and survey analyses. Topics for the briefs are based mainly on those submitted as requests through our members' Research Request Service. Read and absorb, then pass on to your staff/colleagues to do the same.

Business Continuity Planning (BCP) definition

Business Continuity Planning (also known as contingency planning, disaster recovery, or crisis management) is the process of planning, preparing, implementing, and testing an organisation's capability to sustain critical business functions when normal operations have been unexpectedly disrupted. Business continuity planning involves the development and implementation of emergency response procedures designed to maintain the continuity of critical business functions along with the timely recovery of disrupted services.

The stage

In the business world risk is ubiquitous, and crises can arise unexpectedly from many quarters i.e., from the failure of critical equipment, computer viruses, exchange rate fluctuations, loss through fire, water damage, terrorism, pandemics, chemical spills, through to extreme natural disasters. Risk is a "wild card" that can be dealt at any time and which may either partially or completely disrupt an organisation's operations and services. For this reason business continuity plans need to be well designed, encompass all of an organisation's critical functions, and be updated frequently. Given the lessons of September 11, Mississippi disasters and the current bird flu threat businesses are being forced through necessity to look hard at the issue of BCP.

Expert Opinion

Business Continuity Planning (BCP)

It is virtually impossible to predict every likely disaster scenario. However, in this regard James Swann from the Community Banker journal cites [1] Steven Lewis the editor in chief of Edwards Disaster Recovery Directory who believed that some banks become too concerned at trying to predict specific disasters. Lewis believed that the best approach was found in examining the results of disasters i.e.:

1. Loss of information
2. Loss of access, and
3. Loss of people

By considering the various possibilities and gauging a wide range of consequences, organisations can take appropriate measures to protect themselves. The construction of a matrix under each of the above categories can be used to document potential threats to business operations. By using the matrix, managers can ascertain the period of time that given areas might be permitted to remain non-operational. It was recognised that certain segments may not need to be brought back on line immediately, whilst others might be considered as essential services.

Jeff Morgan, chief operating officer of the Futures Industry Association, Inc., and Bob Mellinger, president of Attainium Corporation, a consulting company specialising in business continuity matters, outlined [2] the following key phases associated with BCP:

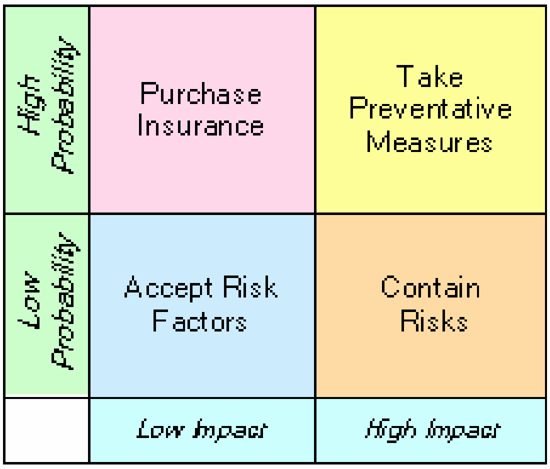
- Preparation for potential disasters;
- Prevention or mitigation of perceived threats;
- Response when crises occur; and
- Recovery from disasters.

Assessing potential risks is a significant challenge and business continuity audits form a useful tool to facilitate such work. The first element of any risk assessment involves considering the likely impact of a disaster upon the organisation's customer services. Mellinger outlines the following three elements used to identify potential risks, their likelihood, and probable impact on day-to-day operations:

1. *Service-Interruption Time Bands* for identifying the time limits for which the organisation can survive without the availability of key business processes e.g. less than 2 hours, 2-24 hours, 24-48 hours, 2-5 days, more than 5 days. Using this process the critical time band for each key process is identified.
2. *Emergency Incident Assessments* for determining which disruptive events are most likely to have the greatest affect upon business processes. This could be achieved by considering unique operational risks, examining each potential disruption, and developing a list of consequences for each threat. Determining the likelihood of each threat and ranking these from 1 to 5 (i.e. very low, low, medium, high, very high) and the possible impact from 1 to 5 (i.e. irritating, controllable, critical, devastating, terminal).
3. *Operational Impact* by combining *Service-Interruption Time Bands* and the *Emergency-Incident Assessment* results. This will identify those areas that are likely to be the most adversely impacted. From this point it is possible to prioritise the various elements of an organisation's business continuity plan. [2]

Risk and Impact Analysis

Ted Udelson president of Integrity Computing [3] writes that business-impact analysis requires the identification of an organisation's critical assets and these may range from "hard assets" such as money and equipment, through to intellectual property and relationships. Impact analysis is used to identify all critical processes and to determine the "value" that the organisation could lose if a crisis interrupted operations. Qualitative analysis is a practical and accessible means of comparing and ranking various possible risks which might affect an organisation. Through understanding which risks could have the *highest probability* of occurring, and which could have the *greatest impact* upon operations, then resources can be intelligently allocated to prevent/recover from these eventualities. For *high probability/high impact risks*, preventative measures can be taken, for *high probability/low impact risks* a containment plan might be employed, for *low probability/high impact risks* insurance could be purchased, and for *low probability/low impact events* the potential consequences might be considered low enough to be accepted. The following matrix derived from Udelson [3] depicts how risks can be categorised in a qualitative manner.



High Probability	Purchase Insurance	Take Preventative Measures
Low Probability	Accept Risk Factors	Contain Risks
	Low Impact	*High Impact*

Carl Kotheimer consultant for Consolidated Risk Management and Bill Coffin managing editor of Risk Management journal [4] describe a risk scoring system which may be used for comparing relative risks and as an aid to evaluation. Three factors are used to arrive at an overall risk score i.e.:

- the potential severity of earnings impairment
- the accountability of management systems, and
- the probability of a loss occurring

Each of these factors is first ranked from 1 to 4, the factors are then multiplied together to produce an *overall risk score*; the higher the score, the more severe the risk, and the greater the urgency to address issues highlighted. The following risk scoring table is adapted from Katheimer and Coffin [4].

Risk Scoring Table	
Rating Factor	Risk Score
Factor A. *Severity*	
- Severe impairment of earnings; survival of business/product line at risk	4
- Short term impairment of earnings; loss of market share or strategic opportunity	3
- Significant shortfall of earnings objectives; future opportunities delayed	2
- Minor inconvenience and loss of earnings	1
Factor B. *Management Systems*	
- No corporate standard for accountability	4
- Corporate standard published but with no consistent accountability for objectives	3
- Some implementation of corporate standards and minimal accountability for objectives	2
- Full accountability for outcomes and objectives with executive compensation tied to results	1
Factor C. *Probability of Loss*	
- High probability of event	4
- Moderate probability	3
- Possible occurrence	2
- Rare occurrence	1

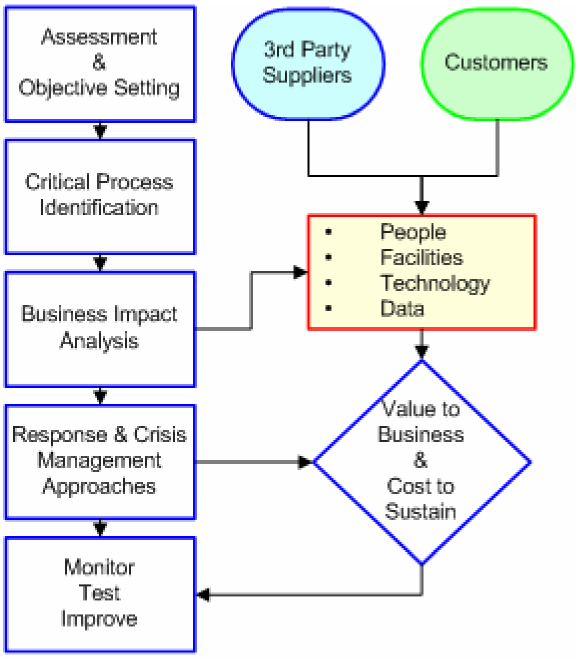
Overall risk score = Factor A x B x C

Practical Emergency Management Plans

Organisations should prepare practical emergency management plans shaped to match their particular needs. Wendy Berliner, Christine Johnston, and Michael Ricciuti, lawyers in the Boston office of Kirkpatrick & Lockhart Nicholson Graham LLP [5] provided the following guidelines for formulating a disaster management plan:

1. Establish a planning team to collect input from all functional areas of the organisation. The team should be given the authority/resources necessary to develop the plan.
2. Analyse the potential hazards and the available resources for combating these hazards. Review current plans and policies along with all applicable laws and regulations. Determine which products, services and operations are vital, and evaluate backups for each of these. Assess the available internal resources (e.g., fire protection equipment, alternative information management systems) and assess the available external resources.
3. Perform an insurance audit to ensure that the appropriate coverage is in place
4. Conduct a vulnerability analysis; by examining the hazards within the organisation and in the local community, considering past crises related to the geographic location, technological weaknesses/threats, or human error.
5. Develop a plan consisting of the following core elements:
   - Direction and control;
   - Communication;
   - Safety human life;
   - Property protection;
   - Community involvement;
   - Recovery and restoration;
   - Administration and logistics.
6. Implement the plan and strive to create a culture of compliance through routine training to keep the plan viable and relevant.
7. Evaluate and modify the plan to ensure that it does not become a static document. Conduct periodic audits to ensure that the plan remains an accurate, realistic and lawful process for the organisation to follow in the event of an emergency. Ideally the disaster management plan should become second-nature to maximise its benefits during an emergency.

Business Continuity Planning should ideally be an enterprise wide exercise for identifying and assessing an organisation's most critical functions. BCP analysis should also take into account the impact of unexpected interruptions upon customers and suppliers along with the ensuing response processes required to restore all critical functions within a prudent amount of time. Eric Krell [6], freelance writer and risk management specialist, provides an overview of BCP processes as depicted in the following diagram:


Assessment & Objective Setting
Critical Process Identification
Business Impact Analysis
Response & Crisis Management Approaches
Monitor Test Improve
3rd Party Suppliers
Customers
People
Facilities
Technology
Data
Value to Business & Cost to Sustain

Testing the Plan

Jonathan Clark head of business solutions and Mark Harman regional managing director, of Crawford and Company International write [7] that effective crisis management planning rests on two principles:

1. *Flexible Decision Making*: Essentially crisis management planning is not about researching and planning for every possible emergency that could occur, but rather about developing the capability to react flexibly and make sensible snap decisions in the event of a crisis.
2. *Practicing*: Rehearsing the type of teamwork that will be required during crises forms a critical component in the development of successful emergency plans.

IT Disaster Recovery

IT Disaster Recovery (DR) plans need to be tested at least once a year or whenever significant changes have been made to hardware or systems. Scheier a writer for Computerworld [8] outlines two basic forms of DR testing:

1. *Desktop walk-through testing*; which involves running through a checklist of responsibilities and actions taken in the event of a disaster. This type of testing is a necessary first step that can help to detect events that could trigger the need for changes to the DR plan.
2. *Live testing*; the most common of which is parallel testing which recovers a separate set of critical applications at a disaster recovery site without interrupting the flow of regular business. The most realistic test of course is a full live changeover of critical systems during working hours to standby equipment. This costly form of testing is rarely used, except for the most critical of applications. Deciding how realistic testing should be involves a balance between the amount of protection desired versus financial costs, staff time, and tolerance to service disruptions.

Scheier advises that it should never be assumed that:

1. All will happen as planned; he suggests that communication problems need to be uncovered by having personnel contact everyone on their contact list in a drill/exercise, and that staff need to be provided with appropriate provisions for potential after-hours work.
2. Data on backup storage devices is current, or that recovery hardware will in fact cope with production databases

Benefits of Business Continuity Planning (BCP)

As well as smoothing the recovery process in the aftermath of a disaster, BCP can add value to organisations through the following benefits outlined by Wayne Clifton [9] director of Risk Control Services for ACE USA Risk Control Services i.e. by:

- Minimising financial loss and embarrassment;
- Retaining customers following an emergency rather than having to find new ones;
- Helping to maintain, or perhaps gain, a competitive edge by offering uninterrupted services;
- Meeting ethical and legal obligations;
- Identifying process inefficiencies and providing an opportunity to assess the effectiveness of the organisations operations and processes and thereby to make improvements;
- Identifying single points of failure and vulnerabilities;
- Helping to maintain confidence among shareholders and customers;
- Protecting jobs and the long term viability of the organisation;
- Providing duplicated resources and back up functions which may also improve the efficiency of daily operations.

Survey and Research Data

IT back-up practices vary widely

A survey of 200 IT managers by Imation in 2005 concerning disaster recovery practices found that the main reasons organisations evaluated their data recovery and back up practices were:
- e-mail viruses (59%)
- Cyber attacks (31%)
- Natural disasters (28%)
- Terrorist attacks (22%)
- Government regulations (19%)
- Employee sabotage (17%)
- Homeland security issues (15%)
- 71% of the organisations surveyed had disaster recovery plans in place
- 40% of companies don't test their disaster recovery plan after each update; and
- 28% percent of companies took a wait-and-see approach.
- 32% performed scheduled testing and evaluation of their storage backup systems at least quarterly and another 35% did so once a year or less. [10]

Crisis Management and communication plans

In reply to a 2005 global IABC Research Foundation survey concerning the preparation of formal communications plans in the event of natural disaster/organisation crises, respondents reported that:
- 30% had no formal plan
- 50% of these unprepared groups needed to rapidly put a plan together in the event of a crisis
- 69% of organisations having a crisis communication plan had needed to implement it, with 53% partially implementing plans, and 47% fully implementing plans.
- Of the organisations that partially implemented their plans, "communication with employees" was the most commonly implemented component (95%), followed by "coordination with other departments or units to determine appropriate communication responses" (93%)
- In regard to the effectiveness of their communication plans; 66% cited the plans as being "very effective," and 33% believed that they were "somewhat effective." [11]

Disaster Recovery (DR) planning – back office operation redundancy (alternative/duplicate systems) valued by banks

The following data was collated from those responding to a 2005 JPMorgan Chase survey concerning disaster recovery planning by US banking organisations:
- 37% indicated that their organisations were well prepared for natural disasters such as hurricanes.
- 55% indicated that they were "somewhat prepared"
- 8% were not prepared
- 50% had either tested their DR plan, or were expecting to do so. The following aspects were valued most in connection with disaster-recovery planning:
- Back-office operation redundancy (72%)
- Communications (68%)
- Offline business operations (65%)
- Corporate communications (58%)
- Employee payroll and emergency funds (49%) [1]

Business Continuity Planning – DR plan testing

In a US Computerworld survey (2004) concerning BCP involving 224 IT managers, respondents replied to the question "when was your organisation's disaster recovery plan last tested?" as follows::
- Less that one month ago (6%)
- 1 to 3 months ago (24%)
- 4 to 6 months ago (18%)
- 6 to 12 months ago (23%)
- More that 1 year ago (10%)
- Don't Know (19%) [12]

Example cases:

Learn valuable lessons from these organisations:

Mississippi Power Co,

Disaster Recovery – empowerment contributes to success

As Hurricane Katrina made landfall all 200,000 of Mississippi Power Co (MPC) customers lost power which remarkably was restored within just 12 days. A high degree of staff empowerment contributed to the successful and rapid restoration. MPC's storm implementation plan provided great flexibility and placed employees into roles that they normally would not carry out. Delegated authority was given to employees in the field to make any necessary decisions to get power restored. Because Katrina had flattened corporate headquarters and disaster response centre MPC's emergency plans were put to the test. Marketing managers and salespeople became logisticians/supply chain managers and all employees assumed clearly defined emergency roles. Many employees had been assigned logistical jobs, or storm assignment, for some time which provided continuity to the plans. The emergency plans were tested about twice a year as real storm conditions threatened services. [13]

Glenmede Trust Co.

Contingency Planning having balance sought

Glenmede Trust Co. tested its disaster recovery (DR) plans seven times per year, and evaluated performance through different disaster levels for various kinds of event. Employees were sent home to test remote working performance. A balance was sought between having a too simplistic DR plan and one that was too complex. Copies of the plan were kept in multiple locations and also included in emergency packs given to staff which contained food, medical supplies, and flashlights. Critical systems could be brought on line within 4 hours using hot standby equipment provided by an outsourcing provider's site. If an incident lasted longer that one week then equipment was available off-site for provision to key personnel. Glenmede appointed a business continuity group which reported regularly to the board of directors. [14]

Ernst & Young LLP,

Crisis Management system tracks worldwide workforce

Ernst & Young needed to protect the firm and its staff and to ensure the continuity of work during disasters and emergencies. E&Y implemented a system to account for its workforce as follows:
1. Employee tracking; All employees were assigned an office and when travelling they always signed in at a nearby E&Y location, even when working at a client's site.
2. Emergency declaration; key crisis representatives at each office had the authority to implement a "roll call".
3. Employee notification; e-mail and voice mail messages were then automatically sent to the employees affected by the emergency event. Employees were able to log onto a Web page, or a national helpdesk to provide key information.
4. Reconciliation; emergency personnel then reconciled records to enable business units to reach out to any staff that had not checked in. [15]

Toronto-Dominion Bank

Crisis Management and handling pandemics

To cover the possibility of a national pandemic the Toronto-Dominion Bank (TD) planned for only 70% of its workforce being healthy and available for work at a given time. A corporate business continuity plan was developed and an associated continuous monitoring system. Critical business functions were identified to ensure that the organisation would continue to function effectively even with limited personnel. Alternative work arrangements were planned to enable employees to continue working during a pandemic, including using multiple back up locations, teleworking, and rotational work shifts. Employees were sent information on how to best protect themselves from infectious diseases and health websites were monitored on a daily basis for possible threats. TD also advised its employees on safe international travel practices and provided information on the company website to counter fear that might accompany a pandemic. [16]

American Century

Business Continuity Planning (BCP) tested in practice

American Century (AC) used a two tier system to provide its workers with secure remote connections for accessing company information i.e.:
1.) Key employees were provided laptops with remote access over a virtual private network.
2.) Another layer of employees with home computers were provided remote access to company applications but not to the complete network. Some 50% of AC's employees were able to work from home. An important consideration using this arrangement was the potential loading on the Internet during a prolonged crisis. American Century designed its

BCP processes by first considering its business requirements, and secondly by providing the necessary technology after practicing various strategies for working through the events remotely. AC had tested the BCP processes by closing down its head office during busy days, and through this process was able to learn valuable lessons and to make refinements. [17]

Measure and Evaluate Business Continuity Planning

In order to fully evaluate the impact of Business Continuity Planning initiatives it is necessary to undertake, where possible, a quantitative assessment of their impact and assign calculable values. The following provide some simple ideas/standards against which BCP effectiveness may be measured/monitored:

Loss/unavailability of information, desired restoration times e.g.:

- Financial records back on line within 2 hours from disruption.
- Customer files back on line within 4 hours.
- Staff locations, status of operations, status of disaster available immediately via mobile phone, Web site, emergency call centre, e-mail.
-

Loss of access to buildings, desired alternative sites established for operations to continue e.g.:

- Alternative sites for business in operation within 2 hours, Home based sites able to operate within 1 hour.
- Information Technology and Communications equipment at alternative sites in operation within 1 hour, or operational immediately using hot standby equipment.
- Key executive and coordinating personnel to be operating from an alternative site within 2 hours
- Front line personnel operational within 4 hours
- Customer service staff operational from home within 4 hours
-

Loss of people, replacement staff to take up roles as follows:

- Key executive and coordinating personnel replacements available within 1 hour
- Field personnel replacements available within 4 hours.
- Customer service replacement staff available within 4 hours.
- Key administrative personnel replaced within 4 hours

Loss of Services, acceptable service disruption period e.g.: minutes, or hours, elapsed from the disruption to full restoration of services. This measure may comprise time bands associated with various services e.g. :

- Time to respond to emergencies: minutes/hours from receipt of advice concerning disaster to initiating resolution.
- Percentage of Services restored within acceptable time span e.g. 80% restored within 2 hours, 90% within 3 Hours, and 100% within 12 hours

Advice to general public/customers, e.g. information released using radio, television, email, Web site, etc concerning the status of the emergency event e.g..

- Expected restoration time e.g. 6 hours, Status update times and sources e.g. every half hour on local radio station.
- Locations where advice and help can be received, e.g. help desk number, Web site.

Summary

Risk is a reality of life with most emergencies being totally unexpected, however by wise Business Continuity Planning organisations need not be unprepared. While it is impossible to predict specific events, it is possible to prepare for certain possibilities which could cause disruptions to an organisation's operations and services. BCP involves making preparations, seeking for means of prevention, and designing recovery processes for responding to business disruptions.

Risk impact analysis is an important component of BCP with loss of information, site access limitations, and the circumstances of people during an emergency, being major areas for consideration. The time frames involved, the degree of service and operational interruptions, along with incident assessment and the consequent responses, all form a part of BCP. Through understanding those risks which might have a higher probability of occurring along with those that could have a greater impact upon an organisation, resources may be intelligently allocated to either prevent, or to recover from, a disaster. Associated with risk analysis is the assessment of the consequences and the acceptability of certain risks.

In responding to a particular emergency the matters which need to be taken into account include:

- Direction and control of personnel and resources;
- Communications between parties;
- Safety of human life;
- Property protection;
- Possible community involvement;
- Recovery and restoration activities along with administration and logistics.

A key component of effective BCP is the testing of plans, modifying them, and making improvements as necessary. The actual details of a given crisis are unpredictable and for this reason staff should be able to react flexibly, within acceptable boundaries, to meet the need on the ground.

BCP has a number of recognisable benefits e.g., the potential to maintain a viable organisation after an emergency, the minimisation of financial losses, holding the confidence of customers/shareholders, and of creating more robust and sustainable organisations.

Note

Techniques and case studies mentioned or summarised in this article can be found in more detail via the BPIR.com along with the full text of most of the articles and reports in the reference list below.

The BPIR Management Brief is a monthly publication delivered as one of the many membership benefits of the Business Performance Improvement Resource (BPIR). To enquire about upcoming Management Brief topics or BPIR membership email membership@BPIR.com or visit the homepage at www.BPIR.com.

Previous issues of the Management Brief:

Vol 1
1 - Work-Life Balance
2 - Ethical Business Practices
3 - Emotional Intelligence
4 - Succession Planning
5 - Managing Innovation
6 - On-The-Job-Training
7 - Motivating Staff
8 - Developing Leadership
9 - Recruitment and Selection
10 - Suggestion Schemes

Vol 2
1 - Customer Satisfaction Surveys
2 - Customer Complaint Resolution
3 - Customer Loyalty
4 - Call Centre Representatives
5 - Customer Relationship Management
6 - Customer Market Segmentation
7 - Customer Knowledge Management
8 - Customer Support and Service
9 - Customer Order Management
10 - Customer Profitability Management

Vol 3
1 - New Product Development & Innovation Strategy
2 - Activity Based Costing and Management
3 - New Product Development - Knowledge Management
4 - New Product Development - Design for Six Sigma
5 - Product Lifecycle Management

References:

The full text of these articles and reports can be found at www.BPIR.com.

1. Swann, J., (2006), **Be Prepared: Crafting and Implementing a Disaster Recovery Plan**, Community Banker, Vol 15, Iss 3, pp 32-36, America's Community Bankers, Washington

2. Morgan, J., Mellinger, B., (2003), **Disaster doctrine**, Association Management, Vol 55, Iss 9, p 26, American Society of Association Executives, Washington

3. Udelson, R., (2005), **What If?A Guide to Disaster Preparedness Planning**, Association Management, Vol 57, Iss 9, pp 67-70, American Society of Association Executives, Washington

4. Kotheimer, C. J., Coffin, B., (2003), **How to justify business continuity management**, Risk Management, Vol 50, Iss 5, pp 30-34, Risk Management Society Publishing, Inc., New York

5. Berliner, W. A., Johnston, C. W., Ricciuti, M. S., (2006), **Essential Disaster Plan Components for Persons Responsible for Human Resource Matters**, Benefit Plan Review, Vol 60, Iss 7, pp 5-8, Aspen Publishers, Inc., Gaithersburg

6. Krell, E., (2006), **Business continuity: creating a framework for success,** CMA Management, Vol 79, Iss 8, pp 30-33, Society of Management Accountants of Canada, Hamilton

7. Clark, J., Harman, M., (2004), **On Crisis Management and Rehearsing a Plan**, Risk Management, Vol 51, Iss 5, pp 40-43, Risk Management Society Publishing, Inc., New York

8. Scheier, R. L., (2004), **A Dose of Reality**, Computerworld, Vol 38, Iss 16, p39, Computerworld Inc., Framingham

9. Clifton, R. W., (2000), **Business continuity planning**, Occupational Health & Safety, Vol 69, Iss 10, pp 178-180, Stevens Publishing Corporation, Dallas

10. Ashton, B., (2005), **Policies, Precautions and Practices**, Computer Technology Review, Vol 25, Iss 3, pp 32, West World Publications, Inc., Los Angeles

11. Holland, R. J., Gill, K., (2006), **Ready for disaster?**, Communication World, Vol 23, Iss 2, pp 20-24, International Association of Business Communicators, San Francisco

12. Scheier, R. L., (2004), **A Dose of Reality**, Computerworld, Vol 38, Iss 16, p39, Computerworld Inc., Framingham

13. Inman, W., (2006), **Staying ahead of the storm**, Industrial Engineer, Vol 38, Iss 2, pp 28-33, Institute of Industrial Engineers, Norcross

14. Robb, D., (2005), **Ready for Trouble?,** Computerworld, Vol 39, Iss 17, pp 25-27, Computerworld Inc., Framingham

15. Anonymous, (2005), **A Plan for Keeping in Touch With Staff and Partners in Case of Disaster**, Accounting Office Management & Administration Report, Vol 05, Iss 11, pp 2-4, Institute of Management & Administration, New York

16. Klie, S., (2005), **One-third of staff could be sidelined by flu, Canadian HR Reporter**, Vol 18, Iss 19, pp 1-2, Carswell Publishing, Scarborough

17. Kramer, L., (2006), **CIO Challenge**, Wall Street & Technology, pp 48-49, CMP Media LLC, Manhasse