BE READY FOR BUSINESS WHEN DISASTER STRIKES

Components of a business disaster preparedness and business continuity plan

By Leonard Jackson, Ph.D., CHRM, CHE, CHTP, CHAE and John Ledgerwood

The aftermath of disasters can be devastating to businesses, especially for those that are not adequately prepared. In fact, research shows that a quarter of all businesses that experience a disaster do not reopen after such events[1]. The numbers are even more daunting for small businesses where as many as 70 percent usually close their doors within a year following a disaster[2]. Seventy-five percent of businesses without business continuity plans are usually forced to close their doors three years following a major disaster[3]. Further, businesses that fail to reopen within 10 days following a disaster are more likely to fail than survive[4].

Conversely, businesses that have well-developed and carefully executed disaster preparedness and business continuity plans are usually able to minimize the impacts of the disasters, and overall costs and losses. Carefully designed plans are cost effective, company specific and address the issues of what should be done to prevent disasters, how to contain the impacts of disasters and how to get the company functioning after a disaster[5].

Disasters are defined as infrequently occurring events that overwhelm the ability of the affected entity to respond effectively to preserve life, safeguard property or maintain the social, economic and political viability of the affected entity[6]. They are classified as either natural disasters or human-induced disasters. Table 1 (page 24) summarizes the most common types of disasters. Business disaster preparedness and planning focuses on taking steps to reduce or limit the effects of disasters on a business[7], and safeguarding life and IT systems[8]. Business continuity on the other hand focuses on restoring the key functions of the business after a disaster, so that it can continue to provide services. For most companies, disaster preparedness and business continuity plans are developed jointly, and usually work in concert with each other. For IT, disaster preparedness planning focuses on a business's computers and its network, with specific emphasis on shifting the infrastructure to back-up sites. While business continuity focuses on identifying business processes that must be restored first[9].

Although some organizations view business continuity and disaster preparedness as the same, others view them as separate processes and documents that complement each other[10]. We'll look at the components of a business disaster preparedness plan and business continuity plan.

Leonard Jackson, Ph.D., CHRM, CHE, CHTP, CHAE is an assistant professor of hospitality resort management at the Fogelman College of Business and Economics, University of Memphis based in Sanford, Fla. John Ledgerwood is an assistant professor of accounting at Embry-Riddle Aeronautical University in Daytona Beach, Fla.

Table 1. Types of Disasters

Human-induced Disasters	Natural Disasters
Accidents	Volcanoes
Crime	Lightning
Cyber crimes	Death of key employees
Strikes	Epidemics
Chemical spills	Earthquakes
Explosions	Fires
Technological breakdowns	Floods
Sabotage	Meteorites
Terrorism	Severe weather conditions
Famine	Tsunamis
Nuclear, biological and radiological threats	Hurricane or typhoon
Riots	Tornado or severe windstorm
Dam failures	Landslide or mudslide
Fires	Electrostatic discharge
Epidemics	Dust contamination

Business Disaster Preparedness

A business disaster preparedness plan is a dynamic document that is developed, practiced and executed to mitigate the effects of a disaster. The document is dynamic since it should be revised to include new business processes since a company changes or evolves over time[11]. The overarching aim of a company's disaster preparedness plan is to prevent disruptions and safeguard assets from physical and psychological threats[12]. Disaster preparedness comprises three components: disaster recovery planning, crisis management and operations recovery[13].

Disaster Recovery Planning. Disaster recovery planning are steps that a business should take to plan for disasters. The recovery plan should start with development of strategies that focus on the safety of the business's most important asset, its people. In addition, each business should ensure that its staff members are trained in how to help the business recover from a disaster. Businesses should therefore simulate different types of disasters and through scenario planning on how to mitigate the effects of a disaster.

Disaster recovery planning should also include the roles and responsibilities of members of the disaster recovery team. The roles and responsibilities of team members usually range from contacting and coordinating the efforts of emergency personnel, to evacuating personnel and safeguarding the company's assets. As part of recovery planning, an alert roster should be developed and executed when a disaster occurs. The alert roster should include the contact information of team members who will be notified when a disaster occurs. The contact information for emergency response agencies should also be included as part of disaster recovery planning.

Disaster planning should also include steps that clearly outline how the disaster should be documented. The documentation should be used to investigate the scope of the disaster and why it occurred.

Another critical component is the steps to mitigate the effects of the disaster on the business. Further, each team member should be responsible for and assigned various steps such as systems shut down, physical asset evacuation, data security and loss prevention. Finally, the recovery plan should include steps towards implementing secondary systems if primary ones are inoperable.

Crisis Management. Crisis management is an essential element of disaster preparedness. It focuses on the company's people and communication with its constituents. The company's crisis management team is responsible for establishing a communication base during and after a disaster to:

- Provide support for the company's employees and their families;
- Assessing the impact of the disaster on the company and its assets;
- Informing the public on the impact of the disaster on the business and the steps taken to recover personnel and the company's assets;
- Contacting stakeholders, including customers, employees, vendors, suppliers, partners, governmental agencies and the media[13].

The crisis management team is also responsible for activating the alert roster and verifying the status of the company's personnel.

Operations Recovery. The final step in disaster preparedness planning is operations recovery. If the company's infrastructure is intact, the company's disaster preparedness team should take steps to restore the company's systems and data to full operation. If facilities or components of the facilities are extensively damaged or destroyed, the company should take steps to purchase or rent facilities or equipment, or relocate operations until the facilities can be restored or acquired. Finally, if the impact of the disaster is such that the survivability of the company is severely threatened, then the company should elevate the disaster recovery process to business continuity which is described in the next section.

Key Components of a Business Continuity Plan

Business continuity planning are the steps that a company should take immediately after a disaster to ensure that its essential functions are restored as quickly as possible so that it can provide its core services to customers. A company's business continuity plan is usually activated in conjunction with the company's disaster response plan if the event is of a magnitude that will cause long term damage to the company's infrastructure. If the business's physical plant or its systems at its plant are inoperable, then the business continuity plan should transfer the company's essential functions at an alternate site.

Developing a Business Continuity Plan. A carefully designed business continuity plan usually follows a series of steps designed to ensure the continuation of business after a disaster[14, 15]. The first step involves conducting an impact assessment of the business to determine the potential impact of various types of disasters on the business and its essential functions. During this step, the company should also determine the amount of time that systems will be unavailable (if a disaster occurs), as well as projected costs.

The next step involves an internal assessment of potential organizational risks and their levels of threats on business processes and systems. Identified threats should be prioritized based on their potential impact on the organization and its constituents. After assessing the organization's risks, the next step should focus on risk management. This step entails developing policies and procedures that cover all business processes. These policies and procedures should outline what steps should be taken to quickly restore all critical business functions. Important and critical vendors should be included in the procedures and steps outlined how to contact them in the event of a disaster.

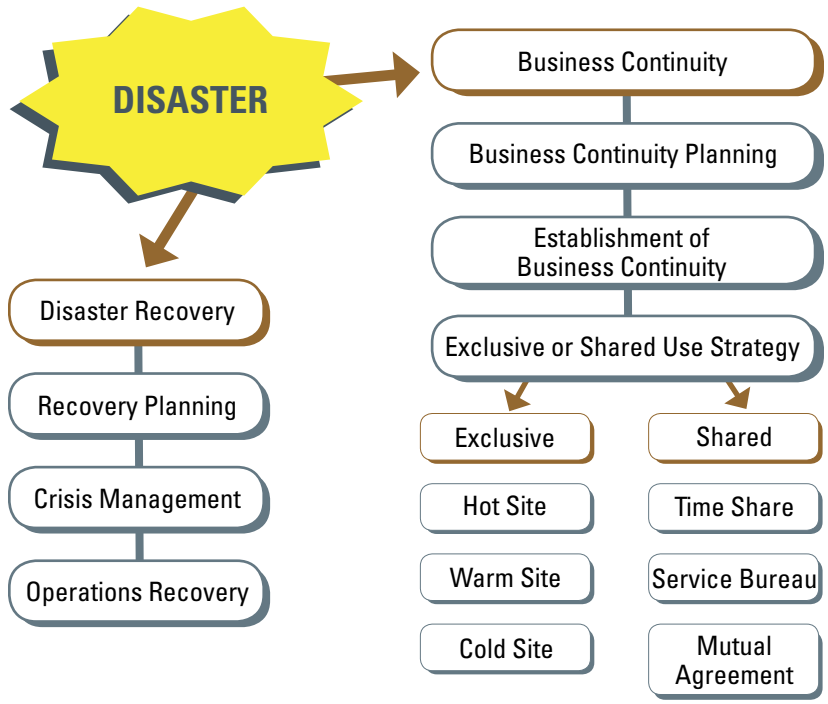
Finally, once the business continuity plan is developed, it should not become a static document. Instead, businesses should execute the next step, risk monitoring. This means that the plan should be tested periodically to ensure that it works, and further that it is current. The plan should also be periodically maintained and updated to ensure currency and that it meets changing organizational needs[14, 15].

Business Continuity Mitigating Strategies. Businesses can select from several types of strategies to ensure continuity following a disaster. The type of strategy a company selects is usually based on its internal costs, distance of alternative facilities from its primary location, accessibility of alternate sites, safety of the alternate location, the level of services provided by vendors and the overall security of alternate sites[16]. In general, a business may select exclusive use option strategies or shared use strategies. Exclusive use strategies are the establishment of hot sites, warm sites and cold sites; while shared use strategies include timeshare, service bureau and mutual agreement.

Hot sites are facilities that virtually replicate all the functions of the business's primary facility. In the event of a disaster that severely affects the critical functions of a business at its primary location, all the company has to do is transfer personnel to this facility and continue operation. These facilities usually comprise duplicates of the company's computing hardware and software, communication systems, peripherals, applications, workstations and up-to-date data, since there is usually real time transfer of data between the primary and the hot site.

Establishment of hot sites ensures that a business can execute its essential functions during a short time following a disaster. However, they are usually costly to maintain. Warm sites have several of the services offered at hot sites including computing hardware, and computing peripherals and servers. However, applications and client workstations are usually not available, so it will take more time for a company to get its operation up and running from a warm site. In addition, a company has to ensure that the hardware at these sites is fully up-to-date and functional at all times, which adds to company

Disaster Recovery and Business Continuity Framework



costs. However, they are usually less expensive to maintain than hot sites.

Cold sites provide the basics for a business to continue its operations. Cold sites are typically an empty building or room without computing or communications facilities. Hence, these items must be installed before the business can continue its operations. The major advantage of cold sites is that they are cheap to maintain, but do take a long time to set up.

Time share sites are sites that are leased and shared by the business and its partners. The major advantage of this arrangement is that operational costs for the facility are shared. However, the disadvantage is that there is the possibility that more than one company within the arrangement might need to use the facility at the same time. Further, the equipment that might be needed by the business might be different from its partners.

Service bureaus are agencies that provide business continuity services for a contracted fee. These companies usually provide data back-up services and will also provide facilities if a disaster occurs. The major advantage of this arrangement is that a company does not have to maintain a facility. However, contracts must be periodically renegotiated with the service bureau.

Mutual agreements or consortiums are arrangements between companies whereby each company agrees to aid the other if a disaster occurs. In this arrangement, the affected business will be provided with essential services, facilities and resources until it is able to recover.

Disaster Doesn't Equal Devastation

Disasters can be financially devastating for businesses, especially small businesses. However, businesses can mitigate the impacts of disasters by developing and executing business disaster preparedness and business continuity plans.

Components of disaster preparedness include disaster recovery planning, crisis management and operations recovery. Business continuity plans focus on restoring the essential functions of a business after a disaster. Business continuity planning includes developing a continuity plan and adopting the appropriate company specific mitigating strategy. Mitigating strategies can be exclusive use strategies or shared use strategies. Exclusive strategies include selecting hot sites, warm sites or cold sites. Shared strategies include time share, service bureaus and mutual agreements. It is advisable that companies select strategies based on costs, logistics and the safety and security of alternative sites. ■

References

1. Open For Business: A Disaster Planning Toolkit for the Small to Mid-sized Business Owner. (2006). Retrieved from http://www.ibhs.org/docs/OpenForBusiness.pdf.
2. Shepstone, D. (2007). National Data Awareness Project Launched to Help Businesses Prevent Data Disasters. Retrieved from http://www.datacentresols.com/news/articles.ful.php?newsid=5455.
3. Blythe, B. T. (2002). Blindsided: A Manager's Guide to Catastrophic Incidents in the Workplace. New York, NY: Penguin Group.
4. Fairbanks, S. (n.d.). How Secure is Your Storage? Protecting Critical Systems and Data with Regular Backup Images and Recovery Processes. Retrieved from http://www.techworld.com/cmsdata/whitepapers/833/How%20secure%20is%20is%20your%20storage_symantec.pdf.
5. Wells, A., Walker, T., Walker, C., & Abarca, D. (2007). Disaster Recovery Principles and Practices (1st Ed.). Upper Saddle River, NJ: Pearson Prentice Hall.
6. Guelke, C. (2005). A Strategic Approach to Disaster Preparedness. Proceedings of the IEEE Engineering Management Conference, Newfoundland, Canada , 2, 745–750.
7. Toigo, J. W. (2003). Disaster Recovery Planning: Preparing for the Unthinkable (3rd Ed.). Upper Saddle River, NJ: Pearson Prentice Hall.
8. Business Continuity Research. (2005). Retrieved from http://www.thebci.org/BCIResearchReport.pdf
9. Panko, R. (2004). Corporate Computer and Network Security. Upper Saddle River, NJ: Pearson Prentice Hall.
10. Nelson, K. (2006). Examining the Factors Associated With IT Disaster Preparedness. Proceedings of the 39th Hawaii International Conference on Systems Sciences, Kauai, Hawaii, 8, 1–10.
11. Morse, G. (2004, June). What's the Plan? A Conversation with Lee Clarke. Harvard Business Review, 1–2.
12. Castillo, C. (2004). Disaster Preparedness and Business Continuity Planning at Boeing: an integrated model. Journal of Facilities Management, 3(1), 8–26.
13. Whitman, M. E., & Mattord, H. J. (2004). Management of Information Security. Boston, MA: Thompson Learning, Inc.
14. Berenfeld, M. (2007, Sept/Oct). Disaster Preparedness: How to Develop a Business Continuity Plan. InfoTech Update, 16(5), 5–6.
15. Strohl, E. (2007). Four Essential Components of a Well-established Business Continuity Plan. Community Banker, 8.
16. Carlisle, V. (2003, August). What is a Business Continuity/Disaster Recovery Plan? Buildings, 43–44.