PREPARATION, PLANNING & PEACE OF MIND

Top Ten Business Continuity & Disaster Planning Tips for Nonprofits

NPower New York

Putting technology know-how in the hands of Non-Profits.

TABLE OF CONTENTS

Introduction

The success of any organization, large or small, depends on many factors. Most importantly, attention and commitment must be focused on sound planning. Proper planning helps ensure that an organization fulfills its mission and meets the needs of its clients. Good business planning must also be based on the amount of resources available at any given time.

But how does an organization plan for the unexpected?

On September 11, 2001, *disaster planning and recovery* took on new meaning for New York City's residents, businesses and nonprofits. No longer were we merely practicing drills or taking preventive measures to mitigate a possible business interruption. We were taking the ultimate test of readiness: reacting to a real-life disaster of unprecedented proportion. Understandably, no one anticipated an event of this magnitude. Organizations learned hard lessons about the importance of adequate planning in the areas of business continuity and disaster recovery. Flaws and gaps in recovery plans were highlighted, many of them major.

Put simply, disaster recovery is the process that takes place during and after a crisis to minimize business interruption and return an organization to its pre-crisis state as quickly as possible. Business continuity is the process of planning and retooling best practices to ensure that the organization survives the crisis. Organizations have now taken a new look at the meaning of "worst case scenario" and use it as a model for good planning. An integral part of this has been to look at how disaster recovery and business continuity plans can complement each other. Naturally, resuming normal operations quickly after a disaster will help minimize disruption and impact. Sound preparation will help make this recovery possible.

NPower NY has compiled a set of preliminary business continuity benchmarks to help the nonprofit executive begin to assess the adequacy of his or her organization's disaster preparedness. Rather than attempting to present a comprehensive look at all aspects of a sound business continuity and disaster recovery (BC/DR) plan, we have created a more general overview of key areas to aid nonprofits in focusing and structuring. With our **Top Ten Benchmarks** as a starting point, we hope to empower organizations by setting them on a path toward the completion of their own detailed BC/DR plans.

We felt this benchmark approach was appropriate because of the number of excellent resources already developed to address comprehensive disaster recovery planning. And since NPower NY's focus is on technology assistance for nonprofits, we also felt it was outside our area of expertise to advise on all aspects of BC/DR planning.

We do realize, however, that most nonprofits are small and have little time to spend on preventive measures that will detract them from their daily work. This speaks to the reality of working in a nonprofit environment. Every day the balance between spending time on preventive planning and service delivery is a delicate one.

In an effort to help the nonprofit community strike this balance, we researched volumes of disaster recovery materials designed for large corporations and consolidated the information to make it more useful to the typical nonprofit. (These materials can be referenced in the appendix at the end of this document.) Once we reviewed the extensive private-sector material, we boiled down our recommendations to a manageable number of tasks designed to help nonprofits begin the process of tightening disaster recovery procedures and plans.

Some of the recommendations clearly relate to technology infrastructure and the security and accessibility of data that resides on computers and related systems. In addition, we included recommendations more generic to disaster recovery. With an eye always toward using technology effectively, we've made recommendations on how technology can help implement these tasks.

Before we included any recommendation in this guide, we measured it against the following criteria:

- The recommendation's successful implementation had to be useful to a nonprofit in its everyday operation, not just in the event of a disaster.

- The recommendation had to be core to a business's comprehensive disaster recovery plan as articulated by the research material we reviewed.

Taken separately, the *Top Ten Benchmarks for Assessing Disaster Recovery Readiness* presented in this document are practical and effective. Collectively, they resonate as a powerful approach to an organization's overall business practice.

How to Use This Tool

The most important thing to keep in mind about this document is that it is not a test.

Rather, it's a tool to be used as a means of assessing your organization's disaster preparedness on a number of critical fronts. It's a way for you to benchmark that readiness against what could be considered best practice.

We hope this guide will help you learn not only about core recommendations but how to implement them in a more sharply defined manner. For example, developing a staff contact list is common sense, and organizations may think collecting this information is enough. But is your list comprehensive, regularly updated, easily retrievable by all staff and able to be synchronized with your handheld device? In the event of a disaster when there is no time to retrieve your files, can you really connect with all of your important parties? One solution, for instance, could be internet services, which are an enormous resource for storing and accessing data from anywhere in the world and can significantly contribute to an organization's recovery.

By recommending technology as a way to facilitate implementation of a business recovery plan, we are not suggesting that technology is a be-all and end-all. It cannot and will not address all of your disaster preparedness challenges. But our research has uncovered the simple fact that the use of technology is often critical in communication and business continuation. We have incorporated some of our own experience into this guide and referenced it in each benchmark's Measurement section.

With any initiative, it is important to empower an individual and/or team to spearhead implementation. For purposes of your organization's business continuity/disaster recovery plan, we highly recommend the appointment of a Business Continuity Champion (BCC). Companies are in the practice of naming fire wardens and searchers to prepare and assist employees during drills and actual emergencies. Similarly a BCC individual or team would be responsible for carrying out preparation, implementation and modification of the benchmarks and related plan. In the event of a possible disaster, the BCC would also serve as the single point of contact for communication, organization, program management and plan execution.

Finally, remember that after completing this guide you have taken an important step in what should be a much more comprehensive examination of your disaster preparedness. This tool will help formulate a critical to-do list, and we urge you to access some of the resources listed in the appendix for additional guidance and follow-up. We hope that by completing this guide and progressing on your own to-do list, you will be ready to undertake a larger BC/DR planning process.

On the following two pages, we've outlined an approach to using this guide and taking the first steps in your business continuity/disaster recovery planning process.

PHASE ONE: GETTING STARTED

It's important to note that not all disasters are beyond our control nor are they usually of the magnitude New York City experienced on September 11, 2001. Disasters can incorporate such events as fire, flood, power outages, theft, system hacking and computer viruses, to name a few. As obvious as it may seem, the best way to prepare for a disaster is to avoid it as much as possible. Therefore, look for any potential problems you can find and begin correcting them. Address those issues that you can solve and which will be beneficial. For example:

Maintain good general housekeeping:

- Keep areas clean and free of obstructions and fire hazards. Consider implementing a clean desk policy. In the same way that a large city phone directory does not burn as easily as loose paper, moving excess papers to file cabinets/repositories at the end of the work day can reduce losses due to fire. It will also help protect documents from sprinkler discharge and other incidents.

- Eliminate any obviously overloaded electrical circuits. Employees may have installed non-business electrical appliances such as coffeemakers, radios, space heaters and fans. These can cause electrical fires by shorting out or overloading circuits not designed for them. Your facilities or building-maintenance personnel may be able to help educate your staff about the problems these appliances can cause. Additionally, ensure your staff is adhering to building-code standards.

Observe physical-security procedures in your facility, and encourage increased security when appropriate. Questions to ask include:

- Are your staff members aware and knowledgeable of their surroundings?
- Is your building open to the public?
- Does your building require ID and access cards?

Observe information-security procedures pertaining to computers in your facility, and encourage increased security when appropriate. Questions to ask include:

- Do staff members have passwords taped to their monitors?
- Are laptop computers secured throughout the workday?
- Are computers protected with up-to-date virus protection software?
- Are your internet sessions protected by company firewalls?
- Do staff members leave computers logged on to the network when they are away from their desks for extended periods such as lunch?

You may not have direct control over some of these items, but you can and should encourage those who do have authority to take appropriate action. Consider security training sessions where appropriate.

PHASE TWO: COMPLETION OF BENCHMARK INSTRUMENT

During this phase, your BCC team and/or individual will: (1) review the benchmarks and related explanations and (2) assess the organization's disaster recovery preparedness against each individual benchmark. After reviewing this document, you will see that a sliding scale and multiple-choice measurements are included to aid in the assessment process. These measurements, also, are not a test: They are guides intended to help you understand where your organization stands in the process of establishing BC/DR best practices.

We strongly recommend that this assessment be done as part of an organization-wide process of BC/DR planning. We encourage you to complete it in the earliest stages of your planning process.

PHASE THREE: BC/DR PLANNING AND IMPLEMENTATION

Once the assessment is finished, the team should examine its results and highlight the organization's disaster recovery strengths and challenges.

After you've had an opportunity to review the assessment data, you'll want to create a short list of critical to-dos designed to streamline aspects of your current BC/DR plan. This list will serve as a roadmap for addressing your identified challenges.

PHASE FOUR: INSTITUTIONALIZATION

The next phase of the benchmarking process involves developing mechanisms for ongoing reflection about your organization's BC/DR practices. The completed benchmark assessment should become a living document that is regularly reviewed and updated by your organization's BCC team. Regular reflection will enable you to modify and revise your technology plan when necessary and to consistently meet your organization's needs.

PHASE FIVE: COMPREHENSIVE DISASTER RECOVERY PLANNING

Once you've made progress on your to-do list, refer to the resources listed in the back of this guide to highlight additional activities and perhaps engage a knowledgeable disaster recovery consultant. For example, you should look at the adequacy of your insurance coverage and ensure that your office has proper emergency-related equipment—*e.g.,* fire alarms, extinguishers and first-aid kits. This is just an example of the many aspects of BC/DR planning that must be addressed to fully prepare your organization.

We hope you find this tool useful. Please feel free to offer your feedback via email at:
information@npowerny.org

Emergency Information

BENCHMARK 1

Document and educate staff on emergency procedures.

Explanation

In an emergency, every second counts. Does your staff really know what to do in an urgent situation? Educate and train employees about appropriate procedures and where to find emergency essentials in the office. Distribute credit card-sized emergency response checklists to employees (what to do, key contacts and phone numbers, etc.).

Establish a chain of command to identify individuals with decision-making authority. They should be selected to coordinate the work of the emergency-response team.

Staff should be aware of the following:

- Location of fire escapes, extinguishers, stairwells and escape routes
- Nearest police precinct, fire station and hospital
- Alarm services
- Flashlights
- First-aid kits
- Emergency contact info (police, fire, building management, etc.)

Measurement

Emergency Procedures

_____ My organization has an updated Emergency Procedures List, distributes it to the staff and provides related training.
_____ My organization has an Emergency Procedures List and trains new staff.
_____ My organization has an Emergency Procedures List but does not train.
_____ My organization does not have an Emergency Procedures List.
_____ My organization waits to have the fire marshal/building management conduct drills.

Accessibility of Lists

_____ Emergency procedures are shared with all staff and are easily accessible.
_____ Emergency procedures are shared but staff is not aware of list location.
_____ Emergency procedures are only shared with executives.
_____ Emergency procedures are not shared at all.

Technology Recommendations

Emergency procedures generally originate in electronic form but are distributed to staff in hard copy. Electronic versions are updated more regularly and should be accessible to staff for easy access and reference. These can be saved as a “PDF” file and stored on your network, distributed via email and/or posted to a secured website. Ensure that the website is accessible to all staff members.

Contact Information/Call List

BENCHMARK 2

Develop a current and readily accessible contact information list for all staff, clients and key vendors.

Explanation

Following an event affecting your organization's ability to do business, the main concern should be about the people who work for and interact with your organization. On September 11, 2001, the importance of maintaining an updated contact list for staff and other important individuals was significantly emphasized. Contacting staff and family members to ensure their safety became paramount. Individuals who need to be contacted generally fall into one of the following groups:

- Employees and family members
- Clients who will be visiting the agency
- Key vendors
- Key clients
- Volunteer staff

When an incident occurs, you may also need to contact some organizations that do *not* fall into any of these categories, such as emergency response agencies. You should create an accessible and comprehensive list of police and fire departments, utility companies and the American Red Cross. If your community uses the 911 emergency-dialing system, be sure to document this information as well as the direct telephone numbers for specific police and fire departments.

Particularly useful in an emergency situation, contact lists are also used daily by organizations that need to connect with staff working in the field or from home. As the use of mobile phones, pagers, email and instant messaging becomes more prevalent, the methods of connecting are constantly evolving.

In some organizations, it may be appropriate to identify team leaders to initiate outreach and recovery options. Maintaining and updating phone trees will also help to communicate more quickly and reduce dependencies on any single person.

Measurement

Contact Lists

_____ My organization keeps comprehensive, centralized and updated contact information on important individuals and groups. Contact information includes home phone numbers, emergency contact information, mobile phone numbers, home email addresses, etc.
_____ My organization collects contact information, but it is not centralized, comprehensive or updated regularly.
_____ My organization does not collect contact information on important groups or individuals.

Accessibility of Lists

_____ Contact lists are shared with all staff.
_____ Contact lists are shared with staff by request.
_____ Contact information is in a locked personnel file available only to human resources and executive staff.
_____ Contact information is not available.

Technology Recommendations

A great deal of contact information is accessible within your human resources or finance and administration systems. Linking this data to a contact system may simplify the creation and maintenance of the list. For example, Microsoft Outlook, in conjunction with the Exchange platform, allows for public access folders. Consider using this tool to store contact information easily accessible to all. Additionally, other email and PDA (personal digital assistant) software includes contact management features. You can create a common contact list and have the information synchronized with your handheld PDA or have it posted electronically to a website, extranet or other electronic platform.

Consider setting up free web-based email accounts, such as Hotmail or Yahoo, as alternatives in the event your primary mail systems are down. Ensure that these secondary addresses/mailboxes are captured in contact lists so they can be accessed as well in the event of an emergency.

Staff may also seek to utilize alternative communication devices such as instant messaging and two-way text pagers in the event of inoperable telecommunication facilities for dial-tone, dial-up access or high-speed connections.

Employee Schedule

BENCHMARK 3

Know the location of personnel during business hours.

Explanation

Have you ever been unable to locate a staff member? In the event of an emergency, it is vitally important to account for and communicate with all staff. Often staff members might be at meetings, seminars or conducting other duties offsite, and communicating with them may be difficult if you do not know their whereabouts. Maintaining a central calendar, complete with contact info, will help you quickly locate and communicate with all staff.

Key items in the list might include:

- Meetings
- Vacations
- Seminars or trainings
- Contact information

Measurement

Employee Schedule List

_____ My organization keeps updated, comprehensive, centralized calendar and meeting schedules for all staff.
_____ My organization collects contact information, but it is not centralized, comprehensive or updated regularly.
_____ Staff maintains individual calendar or meeting information.
_____ My organization does not collect calendar or meeting information.

Accessibility of Lists

_____ Schedules are shared with all staff.
_____ Schedules are shared with specific staff.
_____ Schedules are shared with executive staff only.
_____ Schedules are not shared.

Technology Recommendations

Most email systems and PDAs have calendar features. One option may be to set up a shared office calendar for use by all staff to log meetings and appointments. If it is not practical to have one calendar, individuals can share their personal calendars electronically. As an added benefit, the information could also be posted to a website, extranet or other externally available resource.

There are many free and fee-based web calendaring services. Yahoo and MSN offer free calendar services much like their web-based email. WebEvent and MH Software offer fee-based solutions. Often you can synchronize your PDA with these services to help keep your information up to date.

Critical Records Recovery Box

BENCHMARK 4

Your organization should have a recovery box where critical information is protected and secured.

Explanation

As a matter of due diligence, organizations should take necessary precautions to protect and secure critical records. Floods, fires and other natural or manmade disasters can destroy important information in short order if it's unprotected. Critical records are defined as any information resources essential to the recovery of your business. They may be paper, microfiche or electronic media such as tapes, CDs or diskettes.

Examples of information that might be classified as "critical records":

- Contracts, insurance papers or other legal documents
- Operating procedures manuals
- Computer system backups (CD-ROMs, tapes, diskettes)
- Key human resource or finance data

When determining critical information, it is important to consider that some information may be accessible via third parties. For example: If you provide legal assistance, documents such as briefs and other official papers may be retrieved from the courts. You must determine whether the time required to obtain these copies offsets the costs associated with maintaining and securing them as part of an emergency recovery process.

After determining what the critical records are, select a method for protecting and/or reproducing the information. Analyze options and perform a cost-benefit analysis to select the best method:

- For computer data, regularly utilize a tape backup solution and perform rotations to an offsite facility.
- For critical records, duplicate the record and store offsite in an alternative location or with outside record-storage companies.
- Consider scanning critical paper documents and storing them electronically on CD or a secured website.
- Consider storing critical documents in fire-resistant safes or cabinets.
- For seldom-used critical documents, consider offsite storage such as a safe deposit box at your bank.

Measurement

Recovery Box

_____ My organization keeps critical records in a secured environment both on AND offsite.
_____ My organization keeps critical records in a secured environment onsite only.
_____ My organization keeps critical records but not in a secured environment.
_____ My organization does not keep critical records in any organized manner.

Accessibility of Critical Records

_____ Critical records are accessible to key staff and board members.
_____ Critical records are only accessible to key staff.
_____ Critical records are only accessible to management.
_____ Critical records are only accessible to one person.

Technology Recommendations

A great way to handle paper-based critical information is to convert it to an electronic format. You can use scanners to create digital images of important documents and store them on your computer network, CDs or other electronic media. You can also assign key words and create indexes that will allow you to search thousands of pages of digital information in seconds.

This information can also be stored in a secured manner on your website or intranet to increase accessibility.

For documents stored offsite, consider creating an electronic inventory or database including storage location, archive date and brief summarization of the documents.

Critical Resource Retrieval List

BENCHMARK 5

Develop a list of key resources to retrieve in the event of temporary access to your office.

Explanation

Though most incidents do not completely destroy an office, you still might not be allowed immediate occupancy in the event of an emergency. Authorities may limit access to your facilities until they determine whether the location is safe. As we witnessed many times after September 11th, staff members were granted access to their offices for 10 to 15 minutes—just long enough to gather a few items.

Create a list of the critical items you would need to retrieve if you were granted temporary access to your office. List items in order of importance. The following information should be included:

- Name of the item(s) to be retrieved
- Location
- Ranking in order of priority/importance
- Comments

Some examples of items you might need to retrieve include: computers, computer disks, critical files, patient records, ledgers, checkbooks and work in process.

Measurement

Retrieval Lists

_____ My organization keeps an updated Retrieval List with name and location of resources to be recovered.
_____ My organization keeps a Retrieval List, but it is not detailed or updated regularly.
_____ My organization does not maintain a Retrieval List.

Accessibility of Lists

_____ Retrieval List is shared with all staff.
_____ Retrieval List is shared with specific staff.
_____ Retrieval List is available only to executive staff.
_____ Retrieval List is not available.

Technology Recommendations

Like all critical information, the Retrieval List should be accessible in many ways. In addition to having a hardcopy, you can store copies of the list on your PDA, website or other electronic information service to ensure access when necessary.

Alternate Meeting Location

BENCHMARK 6

Designate an emergency meeting and/or operational location if your primary location is unavailable.

Explanation

In the event your office becomes unavailable due to an emergency, you should designate a location as a meeting place. Make sure staff members are aware of the location and how to get there. This pre-defined meeting place will serve as a location to plan your response to the incident and, depending on your needs, may be used as an initial meeting place or temporary office space. Issues to consider when selecting an alternative space include but are not limited to:

- **Location:** Consider a location relative to your normal workplace. The location should not be so far away that it's complicated for staff to get there. However, it should not be close enough to your office to be affected by the same incident.
- **Communications:** Since communication is central in any crisis response, make sure the location is adequately equipped. If you have mobile phones, pagers, two-way communicators or laptops, try to bring them to the site.
- **Capacity:** Make sure the location has sufficient space to allow for emergency operations (*i.e.,* workspace, facilities, etc.).
- **Security:** Your alternative location may have security restrictions. Be well briefed about any security and/or access issues that may affect the use of the space.
- **Duration:** Ensure the availability of your alternative space. Consider reserving the location for longer than you anticipate. Make arrangements if re-location is necessary due to time/calendar restrictions.

One possible option is to establish reciprocal agreements with other agencies to temporarily share space in the event a primary location is not available.

To help ensure your business practices continue as normally as possible, also be sure your key contacts (clients, vendors, contractors, etc.) are aware of your alternative location and contact information. Consider changing your voice-mail messages to relay the temporary location and telephone reach numbers.

Measurement

Alternate Meeting Place

_____ My organization has a designated meeting space that will allow for emergency operations for all staff.
_____ My organization has a designated meeting space that will allow for emergency operations for executives only.
_____ My organization has a designated meeting space that will allow for limited operations.
_____ My organization has an e-meeting location [see Technology Recommendations below].
_____ My organization does not have a designated meeting space.

Accessibility of an Alternate Meeting Place

_____ All staff members are knowledgeable of the alternate meeting space, how to get there and its accessibility.
_____ Only certain staff members are knowledgeable of the alternate meeting space and its accessibility.
_____ Staff does not have knowledge of the alternate meeting space or accessibility.

Technology Recommendations

E-meeting is an innovative solution that includes the use of electronic, web-based meeting services rather than physical locations. This offers greater access to more people and helps mitigate travel and security concerns. There are many web-based services and application service providers (ASPs) who offer e-meeting and virtual community services. See Appendix: E-Meeting/Virtual Collaborative Information.

Resources Required Over Time

BENCHMARK 7

Develop a list of resources required in the event of a prolonged absence from your location.

Explanation

Many organizations were unable to return to their offices for many weeks, even months, after September 11th. In the event your primary location remains unavailable for a period of time, you may need to plan for additional resources to maintain limited operations. If you are forced to relocate for one to two days, you might be able to maintain partial operations with minimal resources. If the displacement is extended, the required resources may increase significantly depending on the service level you need to maintain.

Plan for the resources you will require for various time frames. Items to consider include:

- Number of staff members in temporary location
- Desks, chairs and basic office supplies
- Phones, printers and fax machines
- Vendor and supplier information
- Computers
- Ability to receive mail
- Money

In addition to identifying what's required, it is also important to identify sources. Talk to your bank, insurance company, vendors or suppliers about their capacity to help expedite delivery in the event of a disaster or disruption.

Measurement

Extended Resource List

_____ My organization has a detailed list of vendors and suppliers necessary to establish limited operations quickly.
_____ My organization has a list of vendors and suppliers.
_____ My organization does not have a list of required resources.

Accessibility of Extended Resource List

_____ Extended Resource List is shared with all staff.
_____ Extended Resource List is shared with specific staff.
_____ Extended Resource List is available only to executive staff.
_____ Extended Resource List is not available.

Technology Recommendations

Consider maintaining an electronic list of critical resources on your organization's shared drive, central database, intranet or secure server. Ensure critical staff has access to the document and has the ability to provide updates and modifications. Also make sure that key staff members maintain a copy of this list on their PDAs or similar devices.

Technical Operations

BENCHMARK 8

Develop a disaster recovery plan for your computer systems in the event of a system failure.

Explanation

As we increase our dependence on information technology and information systems (IT/IS), it is critical to ensure that computer and related systems are protected and can be quickly restored if damaged. You may recall the story of a certain trading firm in the World Trade Center whose computer systems were completely destroyed on September 11th. Within three days, their systems were fully operational at a new location. How were they able to do this after such a disaster? They had an effective computer disaster recovery plan in place.

For computer data and records, be sure to have proper backup AND recovery systems in place—and store the backup offsite! This may be the single most important step you can take to empower your organization to recover from a disaster. The following processes should be implemented:

- **Data Backup:** All computer and server-based data is backed up regularly.
- **Equipment Configuration:** Detailed network documentation and images of all servers, for example, are captured and stored on bootable tapes both on and offsite.
- **Vendor and Client Agreements:** Agreements are stored in a central onsite location with copies stored offsite.
- **Media Inventory:** All software media are inventoried and stored in a central software room with copies of critical media stored offsite.
- **Password Documentation:** User and application passwords and access information are documented.
- **Server Room(s):** Critical equipment is housed in areas with restricted or limited access. For larger spaces, it may be appropriate to have environmental controls in place, such as water and fire protection.
- **Uninterrupted Power Supplies:** All critical equipment must be protected from power outages and surges. This includes network devices, servers, key workstations and telecommunications equipment. Also be sure to surge-protect all equipment connected through phone lines since a power surge through a telecommunications facility can destroy an entire computer through a connected modem.

Suggested Approaches

IT/IS disaster recovery is a complex issue and requires a great deal of attention. One of the most important aspects in disaster recovery is data restoration. Many organizations assume that since they have a backup tape, they can restore. This is a false assumption. Recovery solutions must be fully tested on a periodic basis to ensure proper operations.

Additionally, consider the effects of retention solutions. How often are your backup tapes over-written? Daily? Once a week? Once a month? It may be wise to increase the duration of retention to ensure that valuable information is not discarded prior to restoration practices in the event of disaster or catastrophe.

Make it a critical part of your routine to regularly backup files. Create, document and schedule backup procedures to occur daily. Consider busy times in the day and adjust your schedule accordingly when utilizing web-servers and other backup resources. Following a standard backup process will ensure your organization is adequately prepared.

Measurement

IT/IS Disaster Recovery Documents

_____ My organization has a detailed IT/IS disaster recovery plan in place and has tested to make sure it meets our needs.
_____ My organization has an IT/IS disaster recovery plan, but we do not test.
_____ My organization has system documentation and operating backup solutions.
_____ My organization does not have documentation but does have backups.
_____ My organization does not have documentation or regular backups.

Accessibility of IT/IS Disaster Recovery Plan

_____ IT/IS plan is accessible to all staff.
_____ IT/IS plan is accessible to key staff and management.
_____ IT/IS plan is accessible to management.
_____ IT/IS plan is accessible to IT staff only.

Technology Recommendations

There are many ways to automate, streamline and enhance the disaster recovery process. Software utilities can be used to automate significant portions of the documentation process. Products such as web-based backup services and ASPs (application service providers) can offer greater security, accessibility and recovery of network services.

Insurance & Liability

BENCHMARK 9

Make sure your organization is adequately covered against potential disasters or interruptions.

Explanation

Immediately following the events of September 11th, it was estimated that business-interruption costs totaled $1.8 billion and building-damage costs reached as high as $30 billion. For those organizations who took the necessary precautions, adequate insurance coverage proved invaluable.

How does your organization fare? Do you have appropriate insurance and liability coverage for the following?

- Property
- Buildings
- Equipment
- Executives
- Employees
- Volunteers
- Intellectual Property, etc.

Would your business be able to function after the loss of such assets and resources? Your organization might be covered under fire and theft insurance, but bear in mind that natural disasters such as floods, hurricanes and tornados can strike without warning. *Preparedness is vital.*

Does the nature of your business require your employees to travel offsite? Are volunteers a frequent entity of your business? Do you own your building or rent from a management company? It is important to talk with your insurance company and discuss the many facets of your organization and understand what is truly covered. Policy terms, conditions and exclusions can differ significantly among different carriers in some types of insurance. The policy with the lowest premium may not always be the best value. On the whole, property, casualty and business-interruption insurance cannot bring a company back into operation, but it can help owners protect their equity.

When planning for insurance and liability coverage, keep the following in mind:

- Make sure your organization has adequate insurance for individuals, information, business continuation/interruption and property.
- Consider whether to include the executive officer/executive director and others under “key person insurance” (KPI).

- Review your coverage for restriction of damages from acts of war and natural disasters.
- Investigate intellectual property coverage.
- Verify that your coverage takes the following into consideration: compulsory insurance, limits of liability, professional liability, insurable risks and uninsurable risks. Inquire about the timeliness of payments for claims.

Measurement

Insurance & Liability Coverage

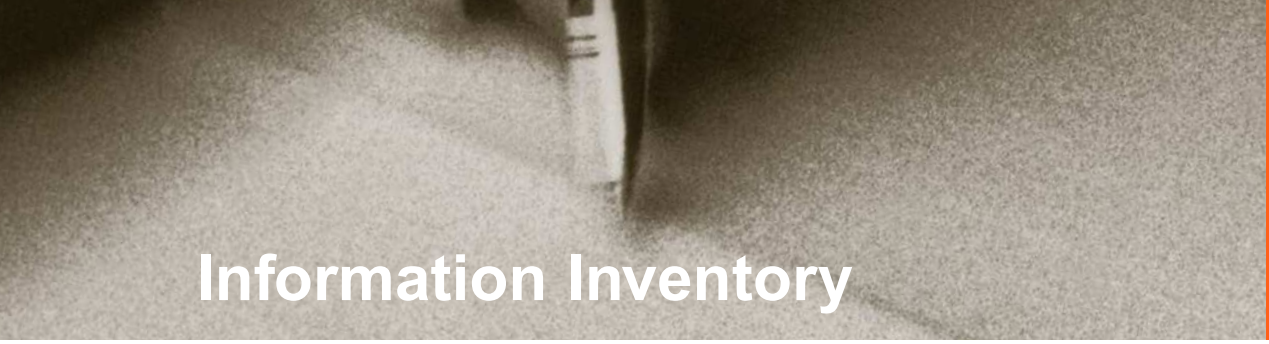
_____ My organization has insurance and liability coverage for all assets, employees and volunteers.
_____ My organization has insurance and liability coverage for assets and employees only.
_____ My organization has insurance and liability coverage for assets only.
_____ My organization has insurance and liability coverage for all types of disasters.
_____ My organization has insurance and liability coverage for specific types of disasters only.
_____ My organization does not have insurance and liability coverage.

Accessibility of Insurance & Liability Coverage

_____ Insurance and liability information is shared with all staff.
_____ Insurance and liability information is shared with specific staff.
_____ Insurance and liability information is available to executive staff.
_____ Insurance and liability information is not available.

Technology Recommendations

Consider maintaining an electronic Insurance Inventory & Liability List on your company's shared drive, central database, intranet or secure server. Ensure that all assets and resources (employees, volunteers, etc.) are listed. Include the policy start dates, expiration dates and extent of coverage for each asset and individual. Ensure that critical staff has access to the document and has the ability to provide updates and modifications. Also make sure that key staff members maintain a copy of this list on their PDAs or similar devices.



Information Inventory

BENCHMARK 10

Develop a checklist that outlines the critical information that is prepared or accessible.

Explanation

As part of the overall approach to preparedness, maintain a checklist of key items that is ready in the event of an emergency. It will serve to document and reaffirm that you have all the relevant information you need. This checklist will cover key areas including:

- **Inventory of Personnel:** Up-to-date home contact information.
- **Key Contacts:** Inventory of vendors and contact information stored on and offsite.
- **Recovery Box:** Protects and secures critical information.
- **Backups:** Inventory of backup completion stored on and offsite.
- **Software:** Inventory of software stored on and offsite.
- **Hardware:** Inventory of workstations, servers, network equipment and telecommunications equipment stored on and offsite.

Measurement

Information Inventory Lists

_____ My organization keeps an updated Information Inventory List and reviews it regularly.
_____ My organization keeps an Information Inventory List but does not review it.
_____ My organization does not keep an Information Inventory List.

Accessibility of Information Inventory Lists

_____ Lists are shared with all staff.
_____ Lists are shared with specific staff.
_____ Lists are available to executive staff.
_____ Lists are not available.

Technology Recommendations

Consider maintaining an electronic Information Inventory List on your company's shared drive, central database, intranet or secure server. Ensure critical staff has access to the document and has the ability to provide updates and modifications. Also make sure that key staff members maintain a copy of this list on their PDAs or similar devices.

APPENDIX—References

Websites on Business Continuity & Disaster Recovery

www.availability.com
A vendor-neutral site committed to the improvement of processes and systems, with informative links to resources to help educate, analyze and remedy business continuity.

www.boardsource.org
Formerly the National Center for Nonprofit Boards. A resource for practical information, tools, best practices, training and leadership development for board members of nonprofits.

www.contingencyplanning.com
An information network providing business continuity and survival strategies, disruption prevention, preparedness, mitigation and emergency response tactics.

www.drj.com
Disaster Recovery Journal has been publishing information on disaster recovery since 1987 and sponsors annual conferences.

www.fema.org
U.S. Government site for emergency and disaster planning/prevention.

www.globalcontinuity.com
A business continuity/disaster recovery (BC/DR) portal service provided by Global Continuity plc. This site has an abundance of information and resources on a broad range of topics.

www.infosyssec.com/infosyssec/buscon1.htm
A comprehensive computer and network-security resource on the Internet for Information System Security Professionals.

www.nonprofitrisk.org
The Nonprofit Risk Management Center offers many free publications on continuity, natural disasters and emergency situations.

www.osha.gov/SLTC/smallbusiness/sec10.html
The Occupational Safety & Health Administration provides an informative site for emergency responses and preparedness.

www.rothstein.com
Disaster recovery information regarding the industry's principal source for hundreds of books, software tools, videos and research reports.

www.sba.gov
The U.S. Small Business Administration site addresses disaster assistance and prevention for small businesses.

www.score.org
Score has numerous local community sites offering small businesses with face-to-face and email counseling for disaster-related events and issues.

Books/Publications on Business Continuity & Disaster Recovery

Business Continuity Planning, 2000 Edition: A Step-By-Step Guide with Planning Forms on CD-ROM, Kenneth L. Fulmer. Available from **www.amazon.com** and other major bookstores.

Definitive Guide to Business Resumption Planning, Leo. A. Wrobel. Published by Artech House, **www.artechhouse.com**.

Disaster Preparedness and Recovery: A Guide for Nonprofit Board Members and Executives, Andrew S. Lang, CPA, and Richard F. Larkin, CPA. Available from Boardsource, **www.boardsource.org**.

Disaster Recovery Planning: Strategies for Protecting Critical Information Assets (2nd Edition), Jon William Toigo. Available from **www.amazon.com** and other major bookstores.

Getting Back to Business—A Guide for the Small Business Owner Following Disaster. Available in PDF format at **www.ibhs.org/business_protection**.

Guide to Business Continuity Planning, James C. Barnes and Philip Jan Rothstein. Available from **www.amazon.com** and other major bookstores.

Manager's Guide to Contingency Planning for Disasters: Protecting Vital Facilities and Critical Operations, Kenneth N. Myers. Available from **www.amazon.com** and other major bookstores.

Open for Business: A Disaster Planning Toolkit for the Small Business Owner. Available in PDF format at **www.ibhs.org/business_protection**.

Primer for Disaster Recovery Planning in an IT Environment, Charlotte J. Hiatt. Available from Idea Group Publishing, **www.idea-group.com**.

Understanding Your Risks: Identifying Hazards and Estimating Losses. Available from the FEMA Publication Warehouse at (800) 480-2520. Request FEMA No. 386-2. **www.fema.org**

Vital Signs: Anticipating, Preventing and Surviving a Crisis in a Nonprofit. Available from The Nonprofit Risk Management Center at **www.nonprofitrisk.org**.

Articles on Business Continuity & Disaster Recovery

"After September 11: Lessons on Planning and Implementing Business Continuity," Charles King. PDF available via the following link: **www.availability.com/research/industry/index.cfm?fuseaction=news&id=C79B2357-6E81-4CBC-8925B65425D3F49C.**

"Business Continuity Planning, a Primer for Management and IT Personnel," John Williamson. Available from the AnyKeyNow Group at **www.anykeynow.com.**

"Business Continuity Lessons Learned from September 11th: A Summary," David Honour. Available from Global Continuity plc at: **www.globalcontinuity.com/default.asp?Art=6219&Type=News.**

"Communicating Out of Crisis," Michael Bland. Available from Global Continuity at **www.globalcontinuity.com/Article.asp?id=37604&ArtId=8813&Type=News.**

"Lessons Learned." Available from the EMC Corporation at **www.emc.com/continuity/lessons_learned.pdf.**

E-Meeting/Virtual Collaborative Information

http://freebies.about.com/library/weekly/aa031299.htm?iam=excite_1&terms=web-based+meeting+service
Overview of free organization methods via online personal information managers and calendars.

http://netconference.about.com/library/weekly/aa041500a.htm?iam=excite_1&terms=web-based+meeting+service
Article outlining the benefits of web conferencing and collaborative options.

http://nonprofit.about.com/library/weekly/aa112800a.htm?iam=excite_1&terms=virtual+community+services
Informative article providing tips on launching a virtual community for nonprofits.

www.conferzone.com/index.html
ConferZone is an objective e-conferencing resource that tracks the latest technology and trends in the marketplace.

www.evolutionb.com
A web-based meeting center for real-time collaboration, including sharing documents and working together on almost any application.

www.eweek.com/article2/0,3959,326382,00.asp
"Web Conference Call." Article is available from the E-Week publication as well as www.eweek.com.

www.groove.net
A peer-to-peer collaboration solution.

www.intranets.com
A web-based meeting center for real-time collaboration, including sharing documents and working together on almost any application.

www.socio.demon.co.uk/vc/toolkit.html
Virtual Community Builder's Toolkit site provides an overview of e-meeting vendor listings, white papers and frequently asked questions.

www.webex.com/home/services_business.html
A web-based meeting center for real-time collaboration, including sharing documents and working together on almost any application.

Acknowledgements

Preparation, Planning & Peace of Mind, Top Ten Business Continuity & Disaster Planning Tips for Nonprofits is made possible through a generous grant from the **JPMorgan Chase Foundation**.

We would also like to acknowledge the following individuals and institutions for their assistance and support in the development of this guide:

Edward H. Pearce, CBCP
Assistant Vice President and Business Continuity Manager
First Services/First Banks

Yihia Mohammad
Zoubir Yazid
Accenture

Norman Meier
Business Protection Systems

Audre Hoffman
Public Entity Risk Institute (PERI)

Dawn Server
City of Longmont, Colorado, Division of Risk Management and Safety

Pat Skahill
Arapahoe County Attorney's Office, Risk Management Division

Credits

Development, Research and Writing

NPower NY
Barbara Chang, Executive Director
David Ritchie, Senior Manager of Project Development
With assistance from the NPower NY staff

Accenture
Andrea Ciurleo

Design, Editing and Production

DDB Bass & Howes

NPower New York
Putting technology know-how in the hands of Non-Profits.

NPower NY
145 West 30th Street, 8th Floor
New York, New York 10001

Phone: 212-564-7010
Fax: 212-564-7009
information@NPowerNY.org
www.NPowerNY.org