Communications, Protection, Readiness (CPR)

NPower's Nonprofit Guide to Business Continuity and Disaster Recovery

CONTENTS

SECTION I: PREPARING FOR THE IMMEDIATE CRISIS RESPONSE

SECTION II: EVERYDAY PRACTICES TO ENSURE RAPID RECOVERY

APPENDIX-References

Underwritten by SBC Foundation

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.

In the fall of 2002, near the first anniversary of the September 11 terrorism attacks on our city and Washington DC, NPower NY, through the support of the JPMorgan Chase Foundation, released the first version of this document. Our goal was to help small to medium sized nonprofits think through basic disaster recovery and business continuity practices. The report was well received by the nonprofit community in New York City and received kudos from our colleagues and fellow nonprofit organizations across the country.

With the support of the SBC Foundation, the philanthropic arm of SBC Communications Inc., we are pleased to update and enhance the document with an eye toward providing new information focused on the technology that can help your organization in its disaster recovery planning efforts. This updated version will complement efforts already underway through SBC's Vital Connections program, which has provided businesses with a list of emergency preparedness tips known as **"CPR" - Communications, Protection and Readiness.**

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 engaging in practice 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 around 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 nonprofit executives assess the adequacy of their organization's disaster preparedness. Rather than attempting to present a comprehensive look at all aspects of a sound business continuity and disaster recovery plan, we have created a more general overview of key areas to nonprofits with focus and structure. With these benchmarks as a starting point, we hope to empower organizations by setting them on a path toward the completion of their own detailed plans. Throughout this guide we will refer to business continuity and disaster recovery efforts and plans as nonprofit CPR (Communications, Protection and Readiness).

We felt this CPR benchmark approach was appropriate because of the number of excellent resources already developed to address comprehensive disaster recovery planning. And since NPower's focus is on technology assistance for nonprofits, we also felt it was outside our area of expertise to advise on all aspects of disaster recovery planning. This new version however, will have a deeper level of technology focus than our first version, and we hope your entire staff, but particularly your IT support staff will find it useful.

Most nonprofits are small and have little time to spend on preventive measures that will distract them from their daily work. This does not mean that nonprofits are irresponsible, but rather it speaks to the reality of working in a nonprofit environment. Every day the balance of 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 of this document and throughout the 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. However, if your organization's mission includes responding during a community crisis, your needs will likely go beyond this document.

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 have 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 had to be core to a comprehensive business disaster recovery plan as articulated by the research material we reviewed.
- The recommendation's successful implementation had to be useful to a nonprofit in its everyday operation, not just in the event of a disaster.

Taken separately, the Top Ten Business Continuity & Disaster Recovery Planning Tips for Nonprofits 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 is a tool to be used as a means of assessing your organization's disaster preparedness on a number of critical fronts. It is a way for you to benchmark your 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 computing 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 solution. It cannot and will not solve 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 Communications, Protection and Readiness Team (CPR team). Companies are in the practice of naming fire wardens and searchers to prepare and assist employees during drills and actual emergencies. Similarly, a CPR team will be responsible for carrying out preparation, implementation and modification of the benchmarks and associated plan. In the event of a possible disaster, the CPR team will also serve as the single point of contact for communication, organization, program management and plan execution.

Finally, remember that after completing this guide you are really just beginning what should be a much more comprehensive examination of all your disaster preparedness activities. This tool may help formulate a critical to-do list, but 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 CPR planning process.

We have outlined an approach to using this guide and taking the first steps in your CPR planning process:

PHASE ONE: Getting Started

It is 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, just 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 themselves 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 their 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 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 encouraging security training sessions where appropriate.

PHASE TWO: Completion of Benchmark Instrument

During this phase, a team of individuals representing a cross-section of the organization is brought together to: (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 CPR best practices.

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

PHASE THREE: CPR Planning and Implementation

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

After you have had an opportunity to review the assessment data, you will want to create a short list of critical to-dos designed to tighten up aspects of your current CPR plan. This list will serve as a roadmap for addressing your identified challenges.

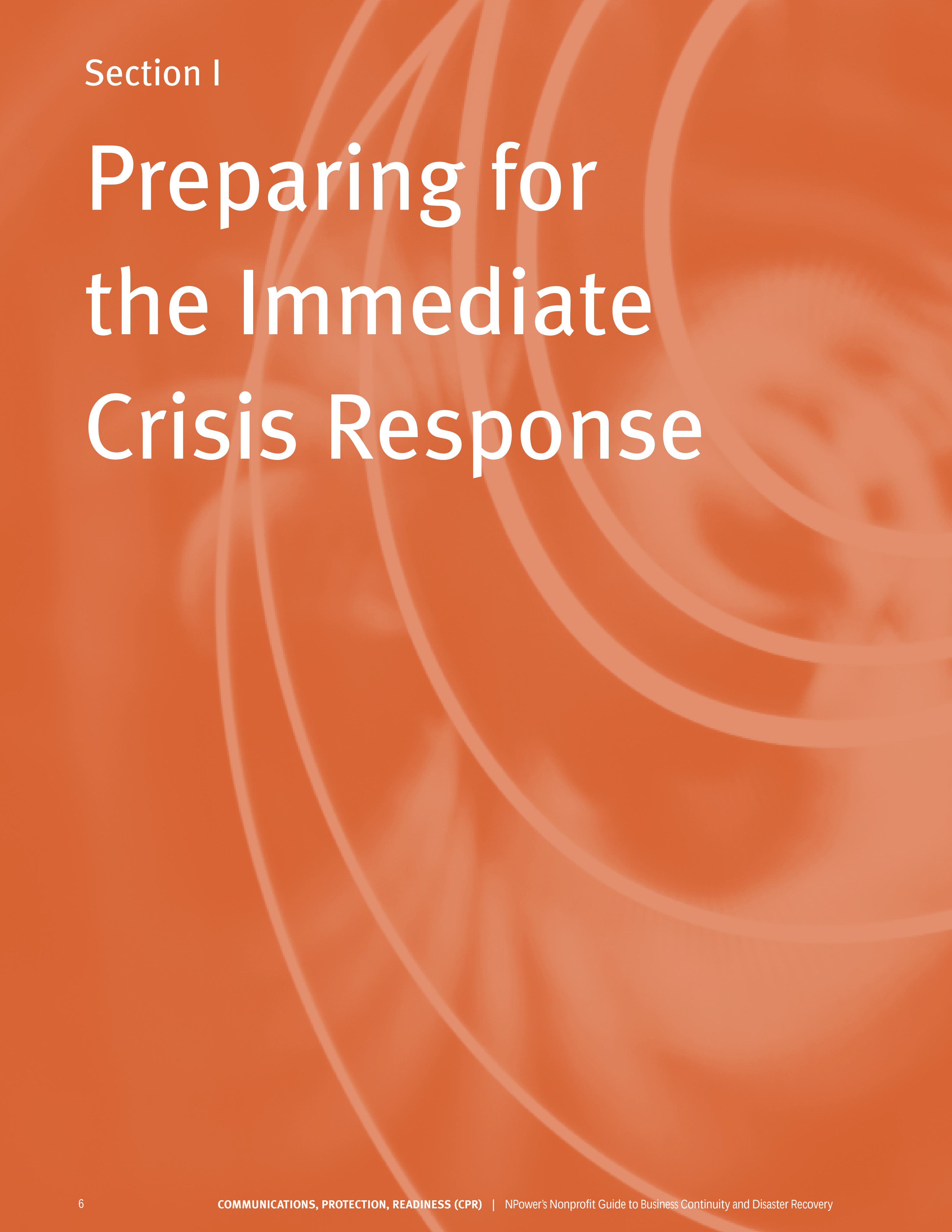
PHASE FOUR: Institutionalization

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

PHASE FIVE: Comprehensive Disaster Recovery Planning

Once you have 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-such as fire alarms, extinguishers and first-aid kits. This is just an example of the many aspects of CPR planning that must be addressed in order for your organization to be fully prepared.

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



Section I

Preparing for the Immediate Crisis Response

Conduct a Business Impact Analysis (BIA)

STEP 01

Explanation

When a prolonged business interruption occurs, whether it is due to a fire, flood, or an extreme case such as terrorism, what do you do? What are the most important activities to engage in to get your nonprofit organization back up and running? Assessing the situation ahead of the disrupting event is what most private sector businesses have done, especially in the wake of September 11th. The chaos that inevitably follows a dramatic event could paralyze an organization's staff for days if not weeks. A Business Impact Analysis (BIA) is the first order of business in thoughtful Disaster Recovery planning.

A business impact analysis (BIA) is a comprehensive study that will help you determine which business processes are critical to your mission. A BIA is the process of analyzing all business functions and the effect that a specific disaster may have upon them.1 Through a thorough BIA exercise, you will be able to determine the type or scope of difficulty caused to your organization should a potential event identified by the risk analysis actually occur.

Only after a BIA is conducted will you be able to make critical decisions about planning for business continuity. A team approach is recommended so that the various key staff and board members within your organization are represented. Your team should understand the infrastructure and processes that drive your mission.

Implementation

The objective of the analysis is to identify which processes and other assets are critical to the ongoing viability of the business. List them and assess their level of vulnerability. Then determine actions to mitigate the negative impact on these assets during a disruptive event.

A BIA includes a review of your facility, processes, systems, equipment and procedures with an eye toward evaluating your ability to continue business operations in the event of a disaster or other interruption. A comprehensive BIA should include a risk assessment, as well as identification of risk prevention activities, and should make specific recommendations as to how to best protect your nonprofit.

For example, a BIA will identify the costs of downtime to your organization.

- Productivity: Each employee unable to work and each hour of lost serviceable time is a quantifiable expense.
- Hampered financial performance: You may be unable to realize revenue, and cash flow can suffer. Without cash on hand there may be an impact on your ability to deliver services.
- Damage to reputation: You can lose equity with all of your audiences— customers, suppliers, funders, business partners and the media when you are unable to perform needed services.
- Other expenses: There are the costs of equipment rental, temporary employees, transportation and other headaches.

Once you have determined the costs of downtime, you probably will find that the cost of developing and implementing a plan will be less than 25 percent of an actual downtime event.

We note that most nonprofits will not have the time or resources to complete a comprehensive BIA. There are many firms that can conduct a BIA for your organization. However, it can cost thousands of dollars depending on the size of your organization. For most large nonprofits this is a critical component to thorough CPR planning, and funds should be set aside to hire a consultant to complete a BIA. Some nonprofits may not have the funds and might want to try a scaled down version of a BIA on their own.

We are highlighting this activity so that at a minimum, you can collect some basic information about the impact of certain mission-critical losses to your organization to help focus limited resources during a crisis.

A basic BIA planning resource can be found at:
http://www.vccs.edu/its/models/bia.htm

Measurement

___ My organization has committed time and resources to completing a comprehensive Business Impact Analysis, and we now understand the impact of a potential disaster on our assets and our organization.

___ My organization has a homegrown BIA, and we are comfortable with what we know and what we don't know.

___ My organization has never conducted anything like a BIA and is unaware of the impact of a disaster on our organization.

[1] Extreme Logic "The Fundamentals of IT Disaster Recovery Planning" 2002

Designate a CPR Team

(Communication, Protection, Readiness)

STEP 02

Explanation

When a crisis hits, who is in charge? Most often staff will turn to the Chief Executive, but what if s/he is not around? Chaos will reign if plans are not made ahead of time, and recovery could take much longer if individuals are not communicating through a central authority.

A chain of command should be established to minimize confusion so that employees will have no doubt about who has decision-making authority in a crisis situation. This chain of command should identify a CPR Team with polices that specify functional groups and group leaders within the team. Within these policies, assign tasks by position rather than by individual to account for employee turnover or unavailability.

Implementation

Staff should be assigned to the CPR team based on their position, skills and experience. Teams should be large enough to remain a viable force should some members be unavailable to respond. Similarly, team members should be familiar with the functions and procedures of each functional group (see below) within the team to facilitate coordination.

The CPR Team should designate functional groups with primary responsibility over a particular area. In addition to playing a coordinating role with overall decision-making responsibility, a well-prepared CPR Team will require some or all of the following functional groups:

1. **Management Group:** Facilitates communications among other teams and oversees IT contingency plan tests and exercises. Locates temporary office space and coordinates activity around its setup.
   Minimum recommended members: Executive Director, Finance Dir/Mgr
2. **Systems/Telecommunications Recovery Group:** Conducts all activities around IT and telecom recovery, as well as data preservation, security and recovery.
   Minimum recommended members: Network Administrator, Telecom Manager, or individual responsible for systems/telecommunications of organization.
3. **Administrative Support Group:** Coordinates activities between and among staff regarding communication with clients, customers, vendors and other parties to ensure continuation of operations.
   Minimum recommended members: Operations Manager, Program Director, Administration Director

Lines of succession should also be included in a CPR Team plan. The order of succession will define who assumes responsibility for the CPR plan execution in the event that the highest authority (usually starting with the ED) is unavailable. For example, if the ED is unavailable, the Finance Director will assume plan responsibility, and if the ED and Finance Director are unavailable, the Operations Manager will assume plan responsibility.

Technology as Tool for Implementation

Equip your CPR team with communication tools that enable short electronic messaging and voice communication. On September 11th, cell phone networks were jammed, and for a short time were completely unavailable. While enhancements to capacity have since been made, email and text messages were able to get through on that day because the messages circumvented the cellular networks, and the amount of information traveling on the Internet was small and compact.

Depending on the type of crisis, different communication tool will be most effective so being equipped with multiple devices is the best bet. Tools (in alphabetical order) that can be utilized by the CPR Team include:

- Blackberry devices
- Cell phones
- Laptop (w/Wireless network capabilities)
- Pagers (two-way)
- PDA (with wireless connectivity)

Measurement

___ My organization has designated a CPR Team with a clear chain of command for when a crisis occurs. The team has clear responsibilities during a crisis situation and is equipped with effective communications devices that can, at a minimum, send short messages within the group.

____ My organization's CPR Team has been designated, but we are still working on clear responsibilities of the team and have not equipped them with any special communication devices.

____ My organization has not yet designated a CPR Team.

Train all Staff on Emergency Preparedness

STEP 03

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 what to do in the event of an emergency and where to find emergency essentials in the office. Distribute credit card-sized emergency response checklists to employees (what to do, key contacts, phone numbers, etc.).

Implementation

While the CPR Team is "command central" during an emergency situation, all staff should be aware of basic protocol, as well as the location of emergency equipment should they need to take quick action. At a minimum, staff should be aware of the following information as part of basic emergency planning and training:

- Location of fire escapes, extinguishers, stairwells and escape routes
- Nearest police precinct, fire station and hospital.2
- Alarm services
- Flashlights
- First-aid kits
- Emergency contact info (police, fire, building management, etc.)

Technology as a Tool for Implementation

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 "PDF" or "DOC" files and stored on your network, distributed via email and/or posted to a secured website for increased accessibility. If at all possible store on more that one secure website at geographically dispersed locations. Ensure that the website is accessible to all staff members.

Helpful Resources

Adobe Free Reader
http://www.adobe.com/products/acrobat/readstep2.html

Microsoft Free Word Viewer
http://download.microsoft.com/download/word2000/wd97vwr/2000/WIN98/EN-US/wd97vwr32.exe

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 staff.
_____ 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.

[2] You should create an accessible and comprehensive list of police and fire departments, utility companies and the American Red Cross. In addition to 9-1-1, be sure to document the direct telephone numbers for specific police and fire departments in your emergency policies in case the 9-1-1 system is overloaded.

Develop Contact Information/ Call List and Employee Schedule

STEP 04

Develop a current and readily accessible contact information list for all staff, clients and key vendors and always know the location of personnel during business hours.

Explanation

One of the first and most important responsibilities of the CPR Team is to contact all staff members to ensure their safety and security. Family members are likely to contact the workplace for the same reason, and the CPR Team should be able to quickly and efficiently determine the status of each individual and communicate that information widely.

Implementation

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 information, will help you quickly locate and communicate with all staff members.

Other important constituencies that will need to be contacted in the short term include:

- Clients who may be scheduled to visit the agency
- Key vendors
- Key clients
- Volunteer staff

Develop a Phone Tree

Beyond contact lists, it is important to develop a rapid method for contacting everyone within your organization. Developing and maintaining a phone tree will help to communicate more quickly and reduce dependencies on any single person. A phone tree involves individuals calling a small number of people, who in turn contact other people and so on until everyone is reached. The phone tree should account for primary and backup contact methods and should discuss procedures to be followed if an individual cannot be contacted.

CPR team leaders should be clearly identified in the phone tree. This contact list should identify team members by their position, name, and contact information (e.g.: home, work, and pager numbers, e-mail addresses, and home address).

Technology as a Tool for Implementation

Setting Up Contact Information

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. Your contact management software may allow 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.

Setting Up Shared Calendaring

Most email systems and PDAs also 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 calendar electronically to make it accessible to others. There are a bevy of shared calendaring products available on the Internet and some even offer a nonprofit discount. These services can be utilized with very little intrusion on your current day-to-day operations and can be synced with your office contact management software. As an added benefit, the group calendaring information could also be posted to a website, extranet or other externally available resource. For more information on shared calendaring options check out http://www.knowledgestorm.com/search/keyword/shared%20calendar%20on%20network/iickwd/Shared%20Calendar%20On%20Network/

Secondary Email Addresses

Consider setting up free web-based email accounts 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 in the event of an emergency. The CPR Team members MUST have alternative email accounts as a precaution. In addition, most cell phones can receive short messages, such as an alert to contact a specific number for more information from team leaders. For more information on choosing the right email service for your organization check out: http://www.emailaddresses.com/guide_types.htm.

Email Protocol

While notifications transmitted via e-mail should be sent, there is no way to ensure immediate receipt. Personal e-mail accounts are sometimes checked as infrequently as once a week. To increase the likelihood that an email will be read quickly, your policies should specify that CPR Team members check personal (back-up) accounts frequently during a crisis. Email notifications should be sent to work email accounts, as well as personal e-mail accounts in the event that the office's Local Area Network is down. Alternative notification tools that are effective during widespread disasters are radio and television announcements and your organization's website.

Call Forwarding

When you are not allowed to occupy your physical office space, you should call forward all calls from your main line to an alternative, accessible line. You may want to explore the call forwarding features available with your voice communications system. For example some systems allow you to use programmable buttons on the phone to activate call forwarding to a pre-determined phone number. You may want to set this up on a CPR Team leader's phone to forward calls from the office to their cell phone or alternative location. If your current voice communications system does not have call forwarding, you should consider upgrading.

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, cellular 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 members.

_____ 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.

Employee Schedules

_____ My organization keeps updated, comprehensive, centralized calendar and meeting schedules for all staff members.

_____ My organization collects schedule and calendar 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 Schedules

_____ Schedules are shared with all staff.

_____ Schedules are shared with specific staff.

_____ Schedules are shared with executive staff only.

_____ Schedules are not shared.

STEP 05

Designate an Emergency Meeting Location for Staff and Command Central for CPR Team

(May be two different locations)

Explanation

In the event your office becomes unavailable during an emergency, you should designate a secondary location where all staff will meet in the immediate aftermath of the emergency. Make sure staff members are aware of the location and how to get there. This predetermined meeting place will serve as a location to plan your response to the incident and, depending on its location and practicality, may be used as a temporary office space.

Implementation

Location of Emergency Meeting Place

Consider a location relative to your normal workplace. The location should not be so far away that it is complicated for staff to get there. However, it should not be so close to your office that it may be affected by the same incident. The location could be a restaurant (e.g. most coffee shops have wireless Internet access for laptops or Personal Digital Assistants (PDAs) which can enable staff to communicate with other staff members remotely. The location should be accessible by mass transportation or ideally, by foot if transportation options are unavailable.

Command Central for CPR Team

During the immediate and short-term aftermath of the crisis, the CPR Team should set up operations in a location that has access to communication channels and that will allow for longer stays. Consider the following when selecting an appropriate location for the setup of the CPR Team:

- Communications: Since communication is central in any crisis response, make sure the location has sufficient communications to meet your needs (e.g. telephones, computers with Internet access, etc.). If you have cell 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 (e.g.., 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 relocation is necessary due to time/calendar restrictions.

Using Technology as a Tool for Implementation

E-meeting

E-meetings are an innovative solution that includes the use of electronic, web-based meeting services rather than physical locations. This may be a vehicle through which geographically disbursed teams can communicate and track progress. This offers 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."

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 above].
_____ 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.

Setting Up Temporary Workplace

STEP 06

Explanation

Your clients depend on you so you need to make sure you plan for a possible relocation during your CPR planning so that you are back in business within days instead of within weeks or months.

Implementation

Nonprofits may want to develop reciprocal arrangements with other nonprofits or business partners to provide recovery capability over the full spectrum of incidents.

CPR Team responsibilities should include a plan to contact key vendors, clients and partners to re-establish communications and gain access to necessary recovery resources. Borrow resources such as office space, supplies or even technology from other business or nonprofit partners to sustain viability. 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 over 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
- Cash

In addition to identifying what is required, it is also important to identify resources. Talk to your bank, insurance company, vendors or suppliers about their capacity to help expedite processing of claims and delivery of new equipment in the event of a disaster or disruption.

Technology as a Tool for Implementation

Recovering Organization Data

In order to access your organization's all-important data during a crisis, a sound recovery strategy must be developed ahead of time. This strategy will depend upon budget and time urgency, among other factors, and can range from simple hardware replacement to more complex mirroring and offsite storage. Several companies can provide services whereby a duplicate real time copy of an organization's data is kept in a secure location offsite. This option is often too expensive for most nonprofits but should be considered if rapid recovery is crucial.

Other recovery methods that could be considered include commercial contracts with hotsite vendors, mobile sites, reciprocal agreements with internal or external organizations, and service level agreements (SLAs) with equipment vendors. For example, an agreement with a vendor or other nonprofit may provide you with access to a conference room with phone access and short term Internet access in which you can create a VPN to your office and can work remotely.

To help ensure your business practices continue as normally as possible, be sure your key contacts (clients, vendors, contractors, etc.) are aware of your alternative locations and contact information. Change your voicemail messages to relay the temporary location and telephone numbers where staff members may be reached and forward all calls to the new location and new telephone number.

Measurement

____ My organization has forged reciprocal agreements with other nonprofits or business partners and has developed a plan to re-establish communications with key vendors, clients and partners.

____ My organization has loose agreements with other nonprofits, and a communications plan is being developed.

____ My organization does not have any agreements, formal or otherwise, and our plans around communications during recovery and business re-establishment are not well-formed.

Section II

Everyday Practices to Ensure Rapid Recovery

Protecting the Lifeblood of a Nonprofit Organization: Your Data

STEP 07

Explanation

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 IT disaster recovery plan in place. 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. Without your data your organization will be paralyzed.

Implementation

For computer data and records, be sure to have a thoroughly tested backup AND recovery system in place-and store the backup offsite! This may be the single most important step you can take to expedite your organization's recovery from a disaster. The complexity of this procedure will depend upon how much data you have, how important that data is to your mission critical activities and what your budget is for securing the most robust backup solution. In some cases, the backup application can be as simple as a file copy using the operating system file manager. In cases involving larger data transfers, an application available through a third-party vendor may be needed to automate and schedule the file backup.

Data Backup

All desktop computer and server-based data must be backed up regularly. If possible all user files should be stored on the main server to ensure that the data gets backed up regularly. If this is not possible or desirable, users should be required to back up the data residing on their PC hard drives on a regular basis. For example CD-ROMs can be used for backing up personal files and are very inexpensive. In addition to backing up data, organizations should also back up system drivers.

With today's ever-changing technology there are several ways of ensuring data continuity. There are ways to backup data including basic tape backup devices, network backup devices and online backup vendors.

Backup Frequency Options

Full Backup: A full backup is done by selecting all the files on the hard disk. Only selected files that shouldn't be backed up at all should be left out. This is the easiest way of backing up your data, but it will take a large amount of time.

Selective Backup: In a selective (or partial) backup, you select certain files and directories to back-up. This type of backup gives you greater control over what is backed up. Selective backups make sense when some files are changing faster than others or when backup space is limited, although in many cases doing an incremental backup is a better and easier option.

Incremental Backup: If you perform frequent backups, as you must, you will find yourself at times backing up the same files often, even ones that do not change over time. Instead, you may want to consider a mix of full backups and incremental backups. An incremental backup is one where only the files that have changed since the last backup are selected. It is similar to a selective backup, but the files are selected based on whether they have *changed* instead of an arbitrary selection based on directory of file names. this gives the time- and space-saving advantages of a selective backup while also ensuring that all changed files are covered.

Media Rotation Options

There are many different media rotation strategies you can use to protect your data.

Backup Strategy: Son (Number of media required: 1 minimum)

The Son scheme simply involves doing a full backup every day. Although the Son strategy is simple to administer, backing up with a single media is NOT an effective method of backup. Magnetic media eventually wears out after many uses. The data you backup is vulnerable on worn media and may not be recoverable.

Backup Strategy: Father/Son (Number of media required: 6 minimum)

The Father/Son media rotation scheme uses a combination of full and differential or incremental backups for a two week schedule. In the Father/Son scenario, four media are used Monday through Thursday for Differential or Incremental backups. the other two media containing full backups are rotated out and stored off-site every Friday.

Backup Strategy: Grandfather (Number of media required: 19 minimum)

The Grandfather method is one of the most common media rotation schemes. In the Grandfather scenario, four media are used Monday through Thursday for incremental or differential backups; another three media are used every Friday for full backups. The remaining 12 media are used for monthly full backups and are kept off-site.

Some backup schedules result in excessive wear on the media that are used most often in the schedule. For example, a schedule may require that the same four media are used to do incremental or differential backups on Monday through Thursday, every week.

The Grandfather/Father/Son strategy eliminates this by rotating media in a way that allows each media to be used the same number of times over a 40 week period.

Data Recovery

Many organizations assume that since they have a backup tape or other media, they can restore their data, but this is a false assumption. Recovery solutions must be fully tested on a periodic basis to ensure proper operations.

In the event of a disaster, newer options allow companies to retrieve their backup data over the Internet (via online back up or Application Service Provider3) and restore it at a Hotsite4 or another company location. Internet backup, or online backup, is a commercial service that allows PC users to back up data to a remote location over the Internet for a fee. A utility is installed onto the PC that allows the user to schedule backups, select files and folders to be backed up, and establish an "archiving" scheme to prevent files from being overwritten. Data can be encrypted for transmission; however, this will impede the data transfer speed over a modem connection. The advantage of Internet backup is that the user is not required to purchase data backup hardware or media.

If access to the Internet is unavailable, backup could occur using a private dial-up network. Hotsite vendors and Internet Service Providers are now offering these services. For more information see: http://www.techsoup.com/articlepage.cfm?ArticleId=198&cg=searchterms&sg=security

Data Redundancy

If your organization has multiple sites with an active directory5, intranet or an application through which critical data is being shared, data backups can occur in various locations. Replicating disk storage either locally or in a remote location is called disk shadowing (when the replication occurs as a result of software resident within a host system), or mirroring (when the replication occurs within a controller or between two controllers that are directly linked).

Another form of local storage redundancy, N+1 redundancy, is called Redundant Array of Independent Disks or RAID. There are various levels of RAID, which match differing workloads, cost, performance, and availability requirements. Local disk shadowing and RAID are very effective methods of guarding against the effects of disk drive failures. Remote disk shadowing will protect files (e.g. should one location lose or destroy its backup tapes or backup storage device.) Preserving redundant data may be too expensive for most non-profit organizations to consider but for larger organizations with sufficient resources, the advantages of redundancy may be worth the cost in terms of quicker recovery time.

Equipment Configuration

Detailed network documentation and images of all servers should be captured and stored on bootable tapes both on and offsite. Imaging will only install the applications and settings, however, and data currently on the disk will be lost. Therefore, PC users should be encouraged to back up their data files separately.

Because servers can support or host numerous critical applications, server loss could cause significant problems to business processes. To address server vulnerabilities, create and strongly enforce server backup polices. (See above section on Data Backup)

To address the local area network (LAN), the physical and logical LAN diagram should be up-to-date. Both diagrams help recovery personnel restore LAN services more quickly. The physical diagram should display the physical layout of the facility that houses the LAN, as well as cable jack numbers. The logical diagram should present the LAN and its nodes. If wireless is being utilized, document the security schema and all associated keys.

Vendor and Client Agreements

Agreements should be stored in a central onsite location with copies stored offsite (see Benchmark #8 Ensure Document Preservation). Vendor names and emergency contact information should be listed in the contingency plan so that replacement equipment may be purchased quickly.

Media Inventory

All backup media should be inventoried and stored in a locked file cabinet with copies stored offsite. It is important that media be retrieved on a regular basis from off-site storage and tested to ensure that the backups are being performed properly and that recovery of data is possible. Each media disk should be uniquely labeled with the date and time of creation so that the most recent data can be identified quickly in an emergency. The agency should develop an effective media tracking strategy, for example a schedule of what media are being held on site and what tapes are at the offsite storage facility.

Organizations should store secondary copies of software and software license information in a secondary location. Custom-built applications installed on desktops should be saved and stored at an alternate location or backed up through one of the methods described above. Instructions on recovering custom-built applications at an alternate site also should be documented, particularly if the application has hard-coded drive mappings (for the PC or network server). Code that prevents the application from running on a different system should be discouraged. If driver mappings are hard-coded, the application should be modified to enable the application to be restored on another system other than the original.

Password Documentation

User and application passwords and access information should be documented and shared with select personnel only. This information should be stored in the critical recovery box (see Benchmark # 8) along with other network documentation.

Server Rooms

Critical equipment should be housed in areas with restricted or limited access and temperature controls. Document configurations of network connective devices that facilitate LAN communication (e.g. switches, bridges and hubs) to ease recovery. For larger environments, it may be appropriate to have environmental controls in place, such as water and fire protection.

Uninterrupted Power Supplies (UPS)

All critical equipment must be protected from power outages and surges. This includes network devices, servers, key workstations and telecom equipment. Also be sure to protect all equipment connected through phone lines with surge protectors as a power surge through a telecommunications facility can destroy an entire computer by way of a connected modem. An Uninterrupted Power Supply [UPS] can protect the system if power is lost. A UPS usually provides 30 to 60 minutes of temporary backup power that may be enough to permit a safe shutdown. A cost-benefit analysis should be conducted to compare a dual power supply and UPS combination to other contingency solutions. Although dual power supplies and UPS are cost-effective for a server, they might not be for a PC.

Network Security

Security on the Internet is a major concern. Hackers and viruses can bring a business to its knees. To prevent unwanted users, from disgruntled employees to hackers, any organization connected to the Internet must have a firewall and/or encryption. Users with dial-up arrangements to your databases must protect their equipment and passwords. Software to detect and remove viruses is available. Proprietary documents or electronic commerce must be secured. There are many new products and services being introduced daily to secure transactions and provide security on the network should be considered in any plan.   For more information check out:
http://www.techsoup.com/articlepage.cfm?ArticleId=90&cg=searchterms&sg=firewall
http://www.techsoup.com/qod_answer.cfm?qotdid=145&cg=searchterms&sg=firewall
http://www.techsoup.com/articlepage.cfm?ArticleId=198&cg=searchterms&sg=security

Measurement

IT/IS Disaster Recovery Documents

_____ My organization has a detailed IT/IS disaster recovery plan in place and has tested it 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.

[3] An Application Service Provider or "ASP" is a technology company that develops and delivers software tools over the Internet, usually for rent rather than outright purchase. These software tools are designed to provide specific services to meet the operational needs of nonprofits and their staff. (source: techsoup.org)

[4] A Hotsite is a facility with all the necessary infrastructure and equipment necessary to enable the rapid recovery of an organization's mission-critical applications. These sites can be housed internally at the organization's facilities, at vendor-provided facilities, or in mobile trailers.)

[5] Active Directory is a centralized and standardized system that automates network management of user data, security, and distributed resources, and enables inter-operation with other directories. Active Directory is designed especially for distributed networking environments.

Ensure Document Preservation

STEP 08

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 man-made disasters can destroy important information in short order if it is unprotected. Critical records may take the form of paper, microfiche or electronic media such as tapes, CDs or diskettes.

Implementation

Examples of information that might be considered "critical records":

- Client records
- Contracts, insurance papers or other legal documents
- Operating procedures manuals
- Computer system backups (CD-ROMs, tapes, diskettes)
- Network Documentation
- 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 retrievable from the courts. Determine whether the time required to obtain these copies from third parties off-sets the costs associated with maintaining and securing them as part of your critical record documents.

After determining what the critical records are, select a method for protecting and/or reproducing the information. 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.

Technology as a Tool for Implementation

Scanning Documents

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. When choosing a scanner consider one with a sheet feeder to expedite the scanning of multiple pages. You can also assign key words and create indexes that will allow you to search thousands of pages of digital information in seconds.

Using Website to Store information

If your website is hosted internally, this information can also be stored in a secured manner on your site. Consider copying the website as a backup and place it on another provider. Also place a copy of the site on your intranet to increase accessibility.

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

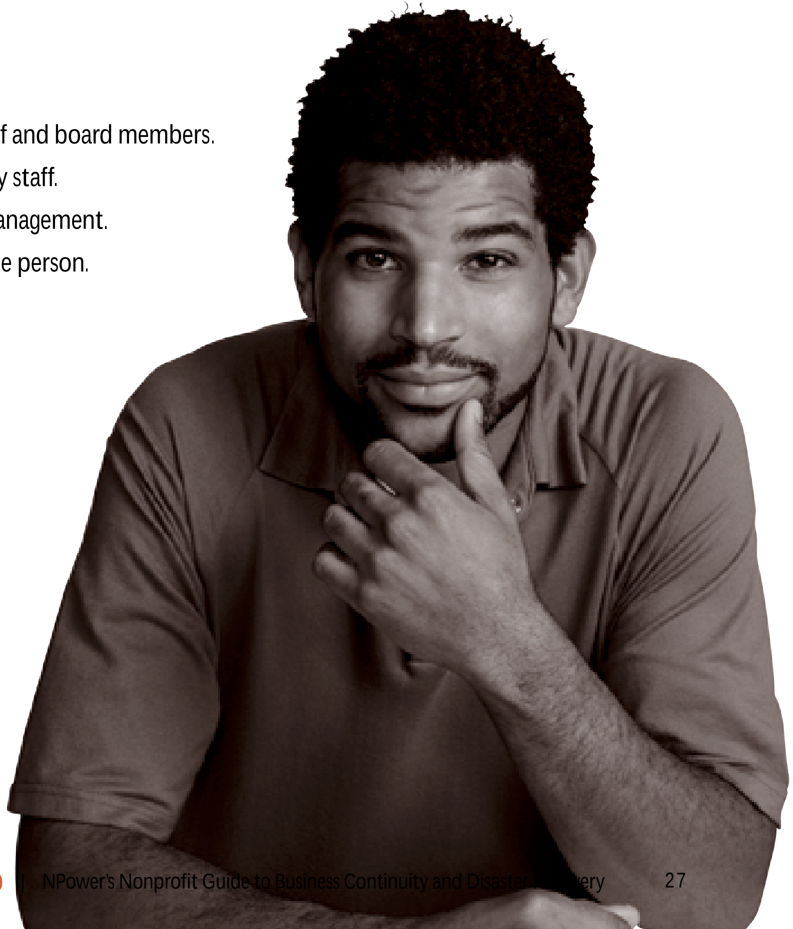
Measurement

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.



Critical Resource Retrieval List

STEP 09

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 might not be allowed immediate access to your office after the crisis has passed. Authorities may limit access to your facilities until they determine that the location is safe. As we witnessed many times after September 11th, staff members were granted access to their offices for as little as 15 minutes at a time-only enough time to gather a few items.

Implementation

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, network documentation, critical files, patient records, ledgers, checkbooks and major works in process.

Using Technology as a Tool for Implementation

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.

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.

Insurance & Liability

STEP 10

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 that took the necessary precautions, adequate insurance coverage proved invaluable.

Implementation

Types of Coverage

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.

Considerations when Securing Coverage

Would your organization 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 may not be covered. Terrorism coverage has recently been added as an option on certain policies. Check your policies and talk to your insurance broker about securing coverage for incidents most likely to cause business interruption in your area.

Does the nature of your organization require your employees to travel offsite? Are volunteers a frequent part of your organization's activities? 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 to 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.

Main provisions to keep in mind when planning for insurance and liability coverage include:

- Making sure your organization has adequate insurance for individuals, information, business continuation/interruption and property.
- Considering whether to include the executive officer/executive director and others under "key person insurance" (KPI).
- Reviewing your coverage for restriction of damages from acts of war and natural disasters.
- Investigating intellectual property coverage.
- Verifying 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.

Ask your insurance agent for more information on these topics.

Technology as a Tool for Implementation

Consider maintaining an electronic Insurance Inventory and 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. Scan images of policies and signatory pages in a secure area of the data network or website. 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.

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.

Appendix

References

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 and 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 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
This site 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.

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

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.

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.
www.globalcontinuity.com/Article.asp?id=37604&ArtId=8813&Type=News

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

We would like to acknowledge the following individuals and institutions for their assistance and support in the development of the two versions of Preparation, Planning & Peace of Mind, Top Ten Business Continuity & Disaster Recovery Planning Tips for Nonprofits guide:

I. Updated Version

SBC Foundation

Curtis Brown, Technology Consultant
Brown Systems

Barbara Chang, Executive Director
Theresa Stroisch, Senior Manager of Training
NPower NY

Jaime Greene, Director of National Services and Knowledge Sharing
NPower

Tari Schreider, Director of Security Practice
Extreme Logic

II. Original Version

JPMorgan Chase Foundation

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

Andrea Ciurleo
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

Barbara Chang, Executive Director
David Ritchie, Senior Manager of Project Development
NPower NY

Communications, Protection, Readiness (CPR):
NPower's Nonprofit Guide to Business Continuity and Disaster Recovery was written by NPowerNY. Questions and feedback regarding this report can be sent to:

NPower NY
145 W. 30th St., 8th Floor
New York, NY 10001
Email us at Information@NPowerNY.org

For more information about the NPower Network, visit our Web site at www.NPower.org or email us at National@NPower.org.