

Business Continuity Planning

November 2003



A Publication of LawNet, Inc.

About LawNet

Providing technology solutions to law firms and legal departments gets more complex every day. Connecting with your peers to exchange ideas with those who have “been there, done that” has never been more valuable.

For over two decades, LawNet has led the way in sharing knowledge and experience for those faced with challenges in their firms and legal departments. LawNet members come from firms of all sizes and all areas of practice, all sharing a common need to have access to the latest information about products and support services that impact the legal profession.

LawNet's Statement of Purpose: LawNet is the premier peer networking organization providing technology information resources to members in order to make technology work for the legal profession.

Editors' Note

“Be Prepared.” Nowadays it’s more than a motto on a sampler—it’s what is driving law firms to invest increasing amounts of time, resources and money in Disaster Recovery and Business Continuity Planning. And if you’re a resident of the earth in this turbulent 21st century, you know all too well why: constant threats of terrorism, catastrophic storms, electrical outages and “cyberharm.” All of these events are uncomfortably recent, and as we’ve learned, any of them can bring a country or community, let alone a single firm, to a standstill.

Being prepared is what this white paper is all about—for everything from a major disaster to less serious events that could detrimentally impact personnel safety and revenue. Our nine authors cover this timeliest of topics in detail—with tips, case studies, disaster scenarios, experienced counsel and good, common-sense advice.

You may be asking yourself, “Is my firm prepared for a disaster?” Now prepare yourself to learn how well from our experts.

Andy Spiegel and Randi Mayes, Editors

Table of Contents

Survival or Loss? Good Disaster/Business Continuity Planning Can Make the Difference	4
<i>by Atlas Lee of Shook, Hardy & Bacon</i>	
Securing Virtual Borders	8
<i>by T. Jason Smith, Esq. of RealLegal, LLC</i>	
BlackBerry to the Rescue	10
<i>by Steve Koontz of Onset Technology</i>	
How Small Firms Can Guard Against “Small” Disasters	10
<i>by Don Philmlee of Potomac Consulting Group</i>	
Data Protection and Recovery: Tips for Successful Planning	11
<i>by Phil Gilmour of EVault, Inc.</i>	
Business Continuation Planning: It's Never Too Soon to Start!	12
<i>by Bob Dolinsky of eSentio Technologies</i>	
Using the Web in Times of Crisis	15
<i>by Maureen Reidy Leuenberger of Hubbard One</i>	
Disaster Recovery Planning: Being Proactive Is Key!	16
<i>by Craig A. Parrish of SSD, Inc.</i>	
Online Backup and Recovery: Overcoming the Trials of Data Protection	20
<i>by Bob Cramer of LiveVault Corporation</i>	



About the Authors

Bob Cramer is CEO of LiveVault Corporation and brings more than 20 years of experience helping companies achieve their business goals by using technology. He is widely recognized as an expert in storage software and application performance management. LiveVault provides fully managed online backup and recovery services for small to medium-sized businesses.

Bob Dolinsky is a Senior Consultant with eSentio Technologies and has more than 20 years' experience in providing technology consulting and management to law firms. His focus includes strategic technology planning, business continuation planning, business process analysis, practice support technology and using technology to enhance client service delivery. He is a frequent speaker at legal industry conferences and a published author.

Phil Gilmour is President and CEO of EVault, Inc., an online data protection software and services provider headquartered in Walnut Creek, Calif. He founded EVault in 1997 after experiencing firsthand the devastation caused by a crashed database. Previously, Phil was Founder and CEO of Benefits Resource Group, a national pension administration firm.

Steve Koontz is the Director of Communications at Onset Technology in Santa Cruz, California, a leading developer of enterprise access software for wireless handheld devices. Steve has considerable experience in all aspects of technical writing, having consulted and managed PR, marketing and technical communications for startup to Fortune 500 companies.

Atlas Lee is Director of Business Continuity for Shook, Hardy & Bacon L.L.P in Kansas City, Missouri. He has been employed by the firm for 15 years and has held several management positions in the IT department. Atlas has over 20 years' experience in computer technology-related areas and 13 years' experience in business continuity planning and disaster recovery. Atlas previously served on the Board of Directors of the Partnership for Emergency Planning based in Kansas City, Missouri.

Maureen Reidy Leuenberger is a Managing Account Director at Hubbard One, a leading provider of software and technology solutions to law firms and corporate legal departments. The company's clients include about 35 percent of the AmLaw 100 and a spectrum of legal departments of large organizations. Maureen is based in Hubbard One's New York offices.

Craig Parrish is the Vice President of Consulting Services at SSD, Inc. He has done extensive disaster recovery and business continuity planning, facilitation and testing for numerous local, regional and national law firms and has extensive facility design and critical systems recovery experience. He has presented workshops on the subject for national, regional and local chapter conferences presented by the Association of Legal Administrators (ALA) and regional and local LawNet groups, and he has had articles published in a number of legal and technology publications.

Don Philmlee is a Partner in Potomac Consulting Group, which specializes in the management, introduction and development of new technology for law firms, including such Internet tools as intranets and extranets, office applications, network and desktop operating systems, multimedia, communications and mobile computing. He has a broad range of experience and expertise working with law firms in many aspects of supporting and managing their technology.

T. Jason Smith, Esq. is a Managing Consultant at RealLegal, LLC, which develops litigation and practice management software for legal organizations and corporations. Previously, he held positions such as Director of Consulting Services and President of Digital Video Operations for legal technology companies. He also consulted on some of the nation's largest trials, working with various Global 100 law firms.

Disclaimer

This report is designed for use as a general guide and is not intended to serve as a recommendation or to replace the advice of experienced professionals. If expert assistance is desired, the services of a competent professional should be sought. Neither LawNet, Inc. nor any author or contributor shall have liability for any person's reliance on the content of or any errors or omissions in this publication.

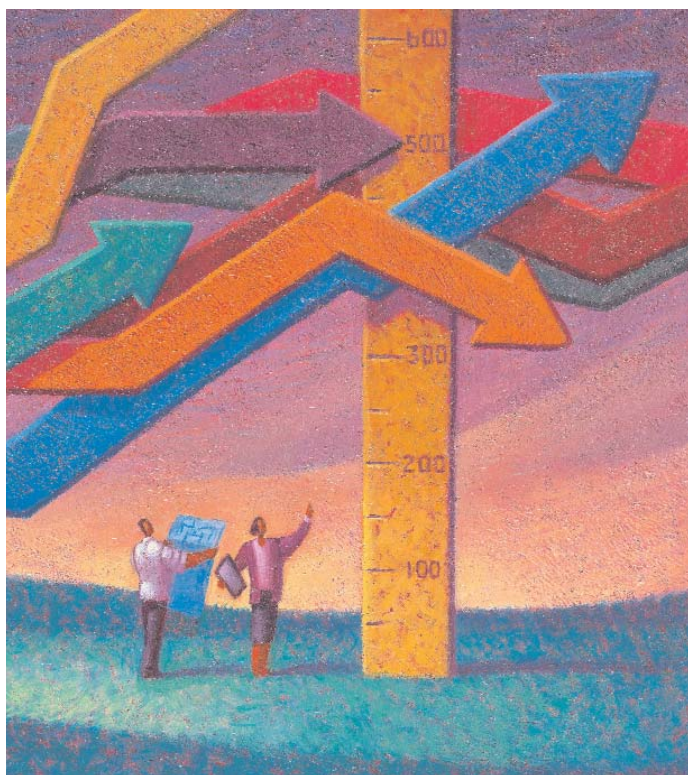
LawNet, Inc., a U.S.-based association, has no connection or affiliation with LawNet Ltd., which is a group of independent law firms operating throughout the United Kingdom and the Republic of Ireland. In the United Kingdom, LawNet, Inc. will be referenced as peertopeer.org. We regret any inconvenience that may have arisen as a result of the use of the name "LawNet, Inc." in the United Kingdom.

Copyright Notice

Copyright © LawNet, Inc. 2003. All rights reserved. Printed in the United States of America. No part of this report may be reproduced in any manner or medium whatsoever without the prior written permission of LawNet, Inc. Published by LawNet, Inc. c/o Andy Spiegel, 2110 Slaughter Lane, #115, PMB 149, Austin, TX 78748.

Survival or Loss?

*Good Disaster/Business Continuity Planning
Can Make the Difference*



In the current economic environment, a company's very existence can depend on downsizing, cost cuts and other measures. Unfortunately, one of the "other measures" often overlooked is the preparation for eliminating or drastically reducing the negative impact of a serious business interruption—in other words, having disaster recovery/business continuity plans and associated processes and procedures.

by Atlas Lee of Shook, Hardy & Bacon

Despite the spate of recent natural and manmade disasters, many organizations still fail to realize the benefits of implementing disaster recovery/business continuity plans, even seem oblivious to the consequences of not having one! Yet, in the normal everyday life of a firm, as lawyers practice law and the support staff keeps things running, there always lurks in the background the threat of a serious business interruption.

How can you protect yourself? Here are some things to consider. But keep in mind that they are general in nature and meant only to stimulate your thinking; they do not comprise a total plan, methodology or formal overview.

Preparedness

In order to respond effectively and efficiently to any business interruption, your plans must be both farsighted and comprehensive. This will help expedite and streamline your response and recovery efforts and minimize chaos within the ranks of the employees. Plus, you can be sure your employees will feel better if they know you are prepared to handle foreseen and unforeseen crises, which in turn will have a positive impact on any business resumption effort.

Preparedness includes doing a business impact analysis to identify what and how much the firm has at risk and which practice and business processes are most critical. You should be prepared, for example, for direct financial impact that can occur due to loss of clients, lost collections from accounts receivable and extended system downtime. The ramifications of an indirect financial impact could translate to loss of clients; loss of key attorneys and employees, even diminished reputation.

As a basic necessity, you will need to do a business impact analysis in order to:

Establish the organizational value of each practice section and administrative department or resource as it relates to the functioning of the firm

Provide the basis for identifying the critical resources required to develop a recovery strategy for the firm

Establish the timely order or priority for restoring functions of the firm in the event of a disruption

A business impact analysis will require the time and effort of senior management and key personnel who are in charge of

critical support departments such as records, accounting, human resources and IT. Input should also come from attorneys or administrators of your practice sections.

A risk assessment identifies the vulnerability of the firm to different categories of risk and its probability. These definitions will help you understand the process of assessing risks:

Probability - The likelihood an event will occur

Impact - Potential consequences or degree of damage, (e.g., revenue loss, adverse publicity, loss of clients)

Exposure - The extent of the impact (e.g., length of time, severity of the issue, frequency of the occurrence)

The risk assessment should include:

Probability of the exposure occurring

Impact to the overall operation of the firm

Financial range of a resulting loss

A determination of cost to eliminate or minimize the exposure

This information should now be used as the basis for making critical business decisions, including:

Tolerance to the exposure

Reducing the tolerance to an acceptable level

Taking the necessary measures to avoid exposure

One person should be responsible for determining what your firm's "acceptable risk" quotient is, but such an important decision should not be made in a vacuum. It requires input from key senior and executive level firm administrators, attorneys and personnel at various levels.

Planning

While you cannot plan for every eventuality—and your employees should be made aware of that—you can identify and plan for the events that are fairly common. Your plans should be:

Comprehensive, yet easy to understand, read and use
Well tested

Inclusive for whichever personnel have specific responsibility for preparation, response and/or recovery. Those individuals should also be responsible for reviewing the plan on a regular basis to make sure the information is timely, and they should each have a copy of the plan or easy access to it. All persons involved in any recovery

process should be aware of their responsibilities and properly trained to carry them out.

Stored in a secure but easily accessible area onsite, as well as offsite.

Proactiveness

Any organization will react to business interruption—the question is, will it be reactively or proactively? Being proactive means that you are confident in being able to deal with an event in a timely and efficient manner. The operative words are "timely" and "efficient." Given that serious business interruptions are now measured in minutes rather than days or hours, reacting proactively to a serious business interruption reaps tremendous benefits, especially in the legal industry in which time is always of the essence. Even though leniency is given by the courts in situations that cannot be avoided, it is not given when a deadline is simply missed without reason.

Protectiveness

Your most valuable resource is your people. Whether they are attorneys, staff personnel or support personnel, your office and building property people should have a set of procedures that address emergency evacuation, bomb and weather-related threats and other potential emergencies. Make sure employees are aware of these and know how to respond accordingly. What happens more often than it should is that organizations and building property management have these procedures in place but rarely use or even practice them because they are "too busy."

Prepare an assessment of employee needs and be prepared to address such "people issues" as shelter, salary continuation, cash advances, incentives and the capability for them to work from home if need be.

Gather volunteers with medical training to assist in medical emergencies and those who can serve as fire/safety wardens. They will be responsible for ensuring that all workers, wherever located, are aware of fire escape routes, evacuation procedures and how to help those who are incapacitated.

Protect your client's assets, both paper and electronic. The latter presents the broader challenge, as there are various ways for do-badders to exploit data, and the invasion can come from inside or outside. Recently we have seen how malicious code can wreck an organization and overwhelm its IT support staff. The fact is, a serious business interruption is more likely to result from the vulnerabilities of a firm's data and networks from viruses, worms, hacker intrusions, denial of service

attacks and the annoyance of spam, workplace violence and civil unrest than from an act of nature.

Sensitivity

If a crisis occurs in the local area of your firm and affects your personnel, you should be prepared for the reality that they will take care of themselves and their families first rather than the firm or organization. Do not base your planning on the expectation that in the event of a disaster your employees will come to work. Some will, of course, but don't count on it—or fault them for it.

You should also be prepared for, and compassionate about, the emotional reactions of your employees to a tragedy. There likely will be such posttraumatic responses as shock, confusion, fear, anxiety and stress disorder. And there will continue to be lingering issues to be addressed by the proper professional agencies; compassion will be a key element in restoring some order of normalcy in the workplace.

Communication

Successful response and recovery from a serious business interruption depend heavily on the ability to disseminate information to your staff and clients quickly and accurately. Measures can include having an up-to-date call tree of all of your personnel and clients, forwarding your phone to a prerecorded voicemail box or remote messaging service, or having a remote voicemail box set up to record messages regarding the operational status of your firm and where employees can retrieve that updated status information. Each employee should have a wallet-sized emergency phone card that contains nonconfidential emergency contact information.

Some organizations may require more sophisticated means of communicating—a formal Command and Control Center that acts as the hub for all operational communications. It could be in a satellite office prewired with additional business phone lines, analog phone lines or DSL lines. It could also be equipped with spare cell phones, satellite phones, two-way pagers and Internet connectivity.

However simple or sophisticated your communication procedures may be, keep in mind that the primary objective is disseminating information to your staff and clients as it becomes available and in an objective, accurate and timely manner.

Another key element regarding communications is to make one person or team solely responsible for addressing the media and/or client base of the firm. And make sure that person is knowledgeable about the communications process so as to avoid mishandling or giving conflicting information.

Practice

They say you must “practice to protect what you need to protect.” I am a witness to this because over the past 10 years I have participated in over 60 full-scale data recovery exercises and a number of tabletop exercises and walkthroughs. It is far better to find out the things that need to be corrected and the areas and issues that need to be addressed *before* you have to respond to a crisis or serious business interruption. This is especially true on the information technology side, given the dynamic nature of technology and associated applications; but it's equally true for the myriad of software patches, updates and new hardware technologies. Don't depend that what worked in a recovery process six months ago will work now.

Practice goes hand-in-hand with being prepared to protect your assets. It should be the norm to practice the evacuation of your office space at least once a year. These drills are normally coordinated with your building management and local police and fire departments.

Other good practice exercises come in the form of walkthroughs. These are exercises coordinated to simulate the reaction to certain scenarios and to validate the viability and usefulness of the disaster recovery/business continuity plans. For instance, how would you respond to a waterpipe break on the floor above a records room, trial preparation room, electrical room or computer room? A tabletop exercise must have at least these components:

Purpose. The purpose of disaster recovery/business continuity exercises is to prove to management the firm's ability to continue to operate to a certain degree in a “business as usual” mode, within a predefined time frame, following a serious business interruption.

Agenda. The agenda of the tabletop exercise should include:

Overview of the exercise objectives

Introduction of the participants and their roles

Practice section/administrative section overview

Description of team plans, processes and procedures

Evaluation of your recovery strategies

Review of corrective actions, issues, and responsible parties

Closing remarks, action items and next steps

Objectives. There must be agreement with all individuals and management participating in the exercise regarding the goals

and scope of the exercise. From a high level, the planning and execution should at least include:

Selection of a facilitator

Selection of scenarios for the exercise

Guidance and direction by the facilitator for walkthroughs

Thorough discussions about plan actions and responsibilities

Notes taken during the exercise with all pertinent issues highlighted

At the conclusion of the exercise the facilitator and participants should discuss issues and comments relevant to the status of the disaster recovery/business continuity planning. It is also imperative that deadlines be set to have any changes to plans made within a reasonable period of time.

Scenarios. For practice, one or two scenarios should be chosen, but they must not be beyond the realm of reality or possibility.

The Downside of *Not Being Prepared*

If everything covered up to this point has not yet convinced you of the importance of establishing a disaster recovery and business continuity plan, here are some of the consequences of not having one, including:

ADVERSE PUBLICITY. It has a negative impact on the perception of a firm, a negative impact on the status of a firm and a negative impact on the working relationship between the firm and its clients. Negative publicity also trigger closer scrutiny of the firm or organization, which in turn can tarnish its reputation.

LOSS OF CLIENTS. Loyalties can become fragile and frayed when your firm can't meet the needs of the client. And when clients become dissatisfied with the lack of serviceability, they will ultimately turn to alternative sources.

LOSS OF REVENUE. Lose a client and you lose revenue. And if the loss is a long-term client who had provided revenue for several years, the firm loses both current and projected revenue.

LOSS OF EMPLOYEES. When the firm loses appreciable revenue, layoffs are a natural byproduct, and that in turn can affect what the firm can pay its employees. This can have a domino effect on the workforce, translating to the loss of "intellectual capital." Those knowledgeable about the day-to-

Any organization that has viable, usable, tested and up-to-date disaster recovery/business continuity plans in place is likely to survive a serious business interruption.

day operations of the firm or with significant experience working on transactional matters or litigation may seek employment elsewhere.

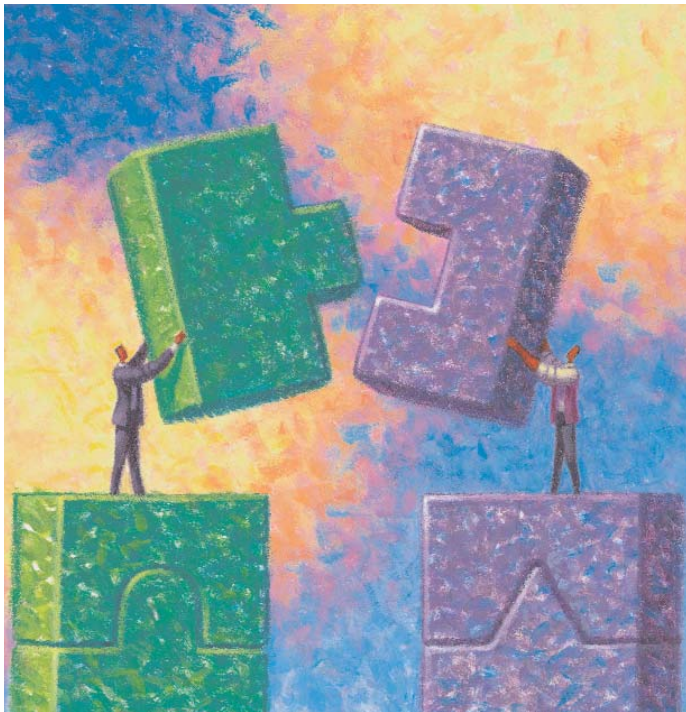
So which sounds better—the benefits or the consequences?

Summary

Today we live in a world that has experienced terrorism, human error and acts of nature, all wreaking more havoc and devastation on humanity and organizations than ever before in history. Sadly and quite possibly there is more to come. But any organization that has viable, usable, tested and up-to-date disaster recovery/business continuity plans in place is likely to survive a serious business interruption. In today's world and economy, survivability is key!

Securing Virtual Borders

by T. Jason Smith, Esq. of RealLegal, LLC



Not so long ago, a virus was an illness and worms were for fishing. Today these are terms used to describe widely distributed computer programs written to exploit security gaps in popular software. At the very least, computer viruses and worms are a nuisance; and at the very worst, they are sophisticated tools used to steal money, trade secrets and personal information or shut down a business or industry for an indefinite period of time. Even more threatening is the use of this technology by fanatics to perform common terrorist activities. Like their counterparts in traditional terrorism who seek weapons of mass destruction, cyberterrorists seek weapons that pose a considerable risk to a society addicted to information.

Casualties of War

In 1999 it was estimated that the Microsoft Windows Operating System comprised 87 percent of all OS sales. Considering the number of vulnerabilities continually found in Microsoft software, this has increased the danger to our world exponentially. Says Sharon Ruckman, Senior Director at the research lab for antivirus vendor Symantec Corporation, “You’re looking at 70 new vulnerabilities every week.”

If terrorists are looking for entry and exploitation points into software used by U.S. organizations, they needn’t look far. Our dependency on technology—and more specifically, our addiction to a single platform—gives rise to single points of failure and abuse. In a June 2002 survey of IT professionals by the Business Software Alliance, 62 percent said the risk of a major cyberattack has increased since 9/11.

On September 23, 2003, the State Department’s computer system, Consular Lookout and Support System (CLASS), which is tasked with checking every visa applicant for terrorist activity, failed worldwide for hours, because of the Welchia virus. CLASS contains more than 12.8 million records from the FBI, the State Department and U.S. immigration, drug enforcement and intelligence agencies—including the names of at least 78,000 suspected terrorists! Welchia is also suspected of shutting down Air Canada’s computer systems.

On the private sector side a single virus attack is costing corporate America billions of dollars. According to Computer Economics, a California research company that keeps track of the projected damage caused by computer viruses, the economic cost of the Code Red worm was nearly \$2 billion in 2001. Network Associates estimated the economic impact of the Nimda virus was roughly \$531 million. These costs include cleanup, resetting security, lost data and lost productivity.

According to the Business Software Alliance, the number of Internet security incidents has nearly doubled each year since 2000. Seventy-six thousand occurred in only the first six months of 2003. While many of these are merely the work of hackers, we understand our nation’s foes use identical technology. If mere pranksters can cause such destruction and loss in terms of data and financial cost, imagine the potential for devastation when terrorists intentionally target infrastructure systems.

Fighting the War

Secretary of Homeland Security Tom Ridge said at the Business Software Alliance Global Tech Summit 2003 (October 9, 2003):

[Some folks] have a notion that homeland security is all about erecting walls and barriers, inspections and intrusions. They see it less an innovation than a necessary evil. Homeland security is about building bridges to one another, even as we build barriers to terrorists. The most important bridges that we build within the Department and then out into the rest of the country, in my mind, are the technological bridges that we build.

The bill that created the Department of Homeland Security gives the government a major role in securing operating systems, hardware and the Internet, including the allowance for more police surveillance of the Internet; up to life in prison for malicious computer hackers; establishing a national clearinghouse for computer and network security work; and spending at least half a billion dollars a year for homeland security research.

But a federal agency can't act alone to protect the knowledge infrastructure of the U.S. Through alliances and partnerships with the private sector, the agency is building an interconnected system of redundancies while educating users at every level to achieve the goal of protection.

Most system administrators probably never expected to be defending the front lines in a global war. In today's technological world, those lines reside inside the walls of our country's most critical organizations, and those administrators are our first line of defense. They help make our technological interdependence strength, not vulnerability.

To secure an organization's technology infrastructure, leading system administrators suggest the following:

Install antivirus software on the server and every computer on the network.

Install a firewall on the network.

Backup software as often as possible—daily is recommended.

Provide basic security training for all system users and advanced training for administrators.

Check for software security updates regularly—at least every seven days.

Provide constant reminders to users of the need to maintain cybersecurity.

Stay on Guard

Cyberterrorism is the “Cold War” of the New Millennium, a genuine threat against our country's infrastructure. IT advancements have strengthened software, system and server security; but at the same time our dependence on technology has increased the risk of danger. While our government, private organizations and individuals examine and implement the latest in protective technology, cyberterrorists are constantly working to infiltrate these systems to disrupt, steal and destroy invaluable data. To prevent and respond to attacks, industries that deal with highly sensitive information are implementing enterprise applications to securely manage their business practices while actively monitoring and auditing access by users.

The ability to protect data and continue working through a crisis can be as important as the ability to recover lost or stolen information.

BlackBerry to the Rescue

by Steve Koontz of Onset Technology

BlackBerry handhelds deliver much more than just e-mail messages. In a disaster scenario when network infrastructure and even cell phone networks are down, the BlackBerry's wireless functionality comes through via PIN-to-PIN messaging. And regardless of wireless status, a BlackBerry can store emergency continuity of operations (COOP) plans and other vital documents for immediate access directly on the handheld.

PIN Updating. If the wireless network is intact, BlackBerry handhelds can communicate directly with each other using device PIN numbers instead of e-mail addresses. The key is to have updated PINs in the handheld's address books (a PIN is not normally included with contact information).

PIN-to-PIN Archiving. Many organizations turn off PIN messaging because of legal requirements to keep records of all communications. But in an emergency PIN messaging may be the only means of communicating. The answer is to archive all PIN-to-PIN messages as the status quo, letting administrators keep the feature turned on in advance of an emergency.

Handheld Document Storage. DR planners need to ensure quick access to contact information, emergency plans and other procedures. A BlackBerry handheld can store hundreds of pages of vital documents (capacity depends on the model) that can be read on the handheld or printed on a fax machine. Documents on a network server are automatically uploaded to handhelds, maintaining the latest versions.

Not all of the above are standard BlackBerry features; some require a third-party application. But the benefit of being able to use BlackBerry deployment as an emergency communication backup can be invaluable.

How Small Firms Can Guard Against "Small" Disasters

by Don Philmlee of Potomac Consulting Group

Much of the today's DR planning is based on methodologies designed for large multioffice organizations. But a disaster recovery plan for a smaller firm with a limited budget requires more creative solutions with less reliance on process and procedures. This does not, however, lessen either the need to plan or the need for policies and procedures.

DR planning can sometimes be too much for a smaller organization with a limited budget. In a smaller organization it's best to plan for the worst kind of disaster. Other lesser disasters can then be considered lesser variants of a total disaster and dealt with creatively by using components from the larger plan.

Some of these technology-based DR examples include:

Creating your own offsite facility by installing a business-class DSL Internet connection at an employee's home

Installing an offsite Web-based backup e-mail server for emergency communication needs (www.convea.com or www.groupville.com)

Setting up AOL / Hotmail e-mail accounts to be used as needed

Backing up files to a commercial Internet storage service (www.xdrive.com)

Making your own Internet Web storage using Windows XP's WebDAV service or a program such as www.webdrive.com

Backing up files to easily restored FireWire drives (www.wiebetech.com)

Getting cooperative agreements to use space at the facility of a client or other firm

Equipping lawyers with laptops so they can synchronize files with the network and always have their work with them (www.mobiliti.com or www.suresync.com)

With a good DR plan and creative solutions, a smaller firm can respond nimbly and quickly to a crisis and keep the work flowing.

Data Protection and Recovery:

Tips for Successful Planning

Today's IT administrators in law offices, faced with unrelenting data growth in accounting, document management and e-mail, find themselves increasingly pressured to ensure the availability and security of their digital assets and to be able to recover quickly from anything from a simple drive failure to a more catastrophic data loss.

But imagine how difficult it is for firms to do this without a formal IT staff—just one person who sets up PCs and swaps out backup tapes while trying to keep up with regular job duties? Strapped for IT resources, these firms often don't set up procedures for how most securely and cost effectively to manage the data backup and recovery processes; rather, they're hampered by such technical limitations as being unable to take advantage of incremental backups that shorten backup windows and enable less data to be stored on spinning disk or tape; having to rely on manual transport of backup tapes instead of leveraging existing network infrastructure where data can be electronically sent to a secure, offsite data center; and if the firm has offices, having to employ a redundant backup infrastructure instead of a centralized one.

For a firm to maintain business continuity, the following—corporate policy, technology and other considerations—should be addressed.

Corporate Policy

Identify, prioritize and protect the company's most important current applications, and forecast which ones will be needed in the future.

As data grows and resources remain static, design a plan that simplifies and automates IT functions. Policy-based automation not only maximizes resources, it limits human errors that, according to the Gartner Group research firm, account for about 40 percent of failures.

by Phil Gilmour of EVault, Inc.

Centralize backup management. Having common practices across offices ensures operational efficiencies related to capital outlay and manpower resources.

Don't recreate backup policies every year for new areas or growing areas. Rather, standardize policies and make them pliable enough to work as the firm and its digital assets grow.

Technology

A data protection and recovery plan requires flexibility to leverage existing infrastructure with cost effectiveness and be able to account for future growth in personnel, amount of data and number of offices.

Other Considerations

Return to Operations. How much downtime can the firm tolerate before it significantly impacts business?

Offsite Storage. If your region has a propensity for natural disaster, does it make sense to get data quickly offsite to a secure data center facility out of the area?

Data Recovery. What are the procedures for getting the digital assets from storage? Who will do this? Identifying and prioritizing business-critical applications will make it easier to decipher what data to restore first.

Security. Does the backup software have a self-encrypting process? Are firewall appliances being used? Consider the owner and location(s) of encryption key(s).

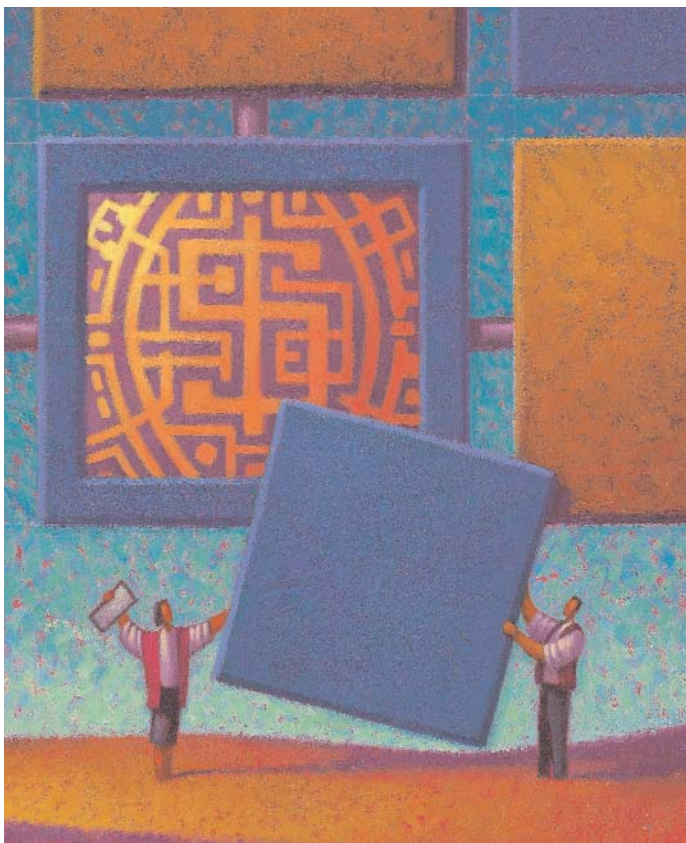
Vendor Evaluation. Look to professionals with a proven track record of helping other firms. Talk to others within your local area. Be cautious of organizations who simply want to throw more equipment at the problem.

By addressing these issues, you will be taking a big step towards establishing a viable data protection and recovery plan—regardless of the size of your firm or IT budget.

Business Continuation Planning

It's Never Too Soon to Start!

by Bob Dolinsky of eSentio Technologies



The catastrophic events of September 11, 2001, brought business continuation planning into sharp focus. But law firms have many other reasons to explore this topic besides the threat of terrorist attacks. Over the past few years firms all over the country have experienced extended interruptions due to electrical outages (Northeast), weather (Miami), earthquakes (Los Angeles), civil disruption (Seattle) and floods (Houston), as well as fire and various building-related issues. And few if any of these firms were well prepared for these events.

Law firms—whose operations are inherently critical—simply cannot tolerate disruptions to their ability to deliver exceptional client service at any time. It is extremely important they be well prepared to avoid unnecessary disruptions—and in the event of one, to minimize the downtime.

Too often law firms develop plans for being able to react to an operational disruption but do not address how to *avoid* disruptions—or at least to minimize their impact on the firm. This article we identify several issues to address that should enable law firms to better arm themselves.

Have an Alternate Site

One cornerstone of effective business continuation planning is to have an alternate processing site available to your firm. The two basic approaches are:

An internal site. You can have another of your offices serve as the alternate site (assuming you have a multi-office firm) or maintain space outside your office(s).

A vendor-provided site. Some vendors offer hot site capabilities; some are only a cold site resource.

Among issues to consider when planning for and implementing an alternate site are:

Hot site or cold site. In a hot site, all the equipment and capabilities you need are ready to go. In a cold site, you have the space and perhaps some of the infrastructure, but you must provide the equipment and support; and you would typically restore your backups when you need the services of an alternate site.

Scope of the technology. In order to support the site, do you need all systems or only those deemed to be a high priority for your firm?

Time. How long will it take you to get the site going and then to restore back to your firm after the disruption?

Space. How much, if any, will be required—not just for the technology but for the use by attorneys and other end users in the firm? Some alternate sites offer workspace, phones, etc. Assess and plan for the type of space you will need and where attorneys and others will work.

Cost. In the end, this is a business decision and must be regarded as such.

Having an alternate site or at least an agreement to have the use of some backup space can substantially reduce the period of a disruption.

Access to Backup Power

Power outages are the most common cause of disruptions to law firm technology. While they're usually relatively brief, they can be substantial, as was the case this summer in the Northeast. Most firms are prepared only for brief outages—but why not plan for the worst? Consider gaining access to your building's backup generator or installing generator capabilities of your own (not an inexpensive option but one worth considering). You needn't cover all of your office space, but at a minimum have enough backup power to cover your key infrastructure (servers, switches, etc.) and some limited workspace for end users.

Some building owners and managers allow firms to have limited output of their backup generators. It pays to ask about and negotiate this into a lease when you are moving or renegotiating your lease terms.

Have an Adequate System Backup Strategy and Procedures

Backups are a cornerstone of business continuation planning, and your approach to doing them can make the difference between a short disruption and a major one.

While this may seem obvious to many in technology management, it's surprising how many firms do not adequately address backup policies and procedures. Make sure that you are focused on the following areas:

Frequency. Backups should be done daily.

Testing. We have seen firms that thought they had good backups, but unexpectedly found otherwise.

Time to restore. This will vary from firm to firm, application to application. Identify your parameters and build your system accordingly.

Storage locations and access. Have offsite storage with 24-hour access.

Scope. All applications should be included.

Commonality. Be sure all backup and restore devices are compatible.

Many firms turn to vaulting technology as their backup methodology. AmeriVault and eVault are two examples of companies that provide this service.

System Security

All too often the cause of disruptions to technology processes is inadequate system security—two of the main culprits being unauthorized access and lack of adequate virus protection. We all know about firms that have gone without e-mail for hours or days due to one of the many viruses or worms that are proliferating. Some of these disruptions to vital communication could have been avoided with up-to-date virus protection and the related policies and system monitoring. Clearly, this is an area on which firms should focus in order to avoid disruptions.

Good system security is important for many reasons—not least, its ability to help minimize the risk of a disruption to operations. Unwelcome intruders can do more than improperly access information; they can cause your firm substantial downtime and expense. Make certain you have adequate security in the form of policies, procedures, hardware and software (including firewalls).

Redundancy in System Design and Technology Infrastructure

All too often, firms have experienced substantial interruptions to service because they did not anticipate system failure. Most of these design problems could have been avoided. Examples of infrastructure issues to assess include:

Having multiple and diverse Internet access points

Having multiple routes and vendors in your WAN design

Avoiding single points of failure in equipment and services

Maintaining reasonable capacity on your WAN

Building automatic failover capabilities into your system where possible

Have an Inventory of Spare Critical Equipment

Maintaining or having quick access to spare equipment is important in minimizing disruptions. Key components break, and the difference between a minor and major outage can be how quickly the equipment or key components can be replaced. Consider stocking backup servers, infrastructure cards and power supplies. Or you may be able to arrange for your vendor to maintain an onsite inventory of key components, which would reduce the cost and management issues related to maintaining your own inventory of spares.

Redundancy also extends to having adequate spare workstations, printers and laptops. If you experience an issue that impacts some or all of your end user workspace, having spare equipment will help get things quickly running again.

Locating Technology Outside of High-Risk Areas

All too often firms locate their technology function in areas of their space without considering potential risks. For example, we have seen firms with water and waste pipes in the ceilings of their server rooms—and more than once we’ve witnessed the unpleasant results when these pipes break. We’ve also seen server rooms that contained sprinkler systems. While in some regions building code may require sprinklers in all areas, including server rooms, modifications can be made to cut the risk of a water-related shutdown. And speaking of water damage, we suggest that you try to avoid locating server rooms on a low floor in a building that is subject to flooding or near outside walls where windows might be vulnerable to storm-related blowouts.

Environmental Controls

One way to avoid disruptions is to ensure that you’re equipped with adequate environmental controls. These include temperature controls, smoke detectors and water detectors (under your raised floors if you have them). Catching problems early can mean the difference between a minor disruption and a major outage.

You should have backups for your key environmental systems, including a backup AC or fans. Many firms keep room-sized fans or portable AC units handy just for this purpose. As in most firms, your primary AC units rely on water for the cooling process; the problem is, if the water goes out in your building you’ll lose your AC. One way around this is a glycol-based cooling system for your key areas. You should also have an adequate fire suppression system and keep it properly maintained.

Documentation

Being able to quickly lay your hands on documentation is also important. The following documents and information should be kept both current and easily accessible:

Maintenance agreements

Firm contact information

Client information

Attorneys and administrative staff information (including PDA PINs where applicable)

Vendor information

Utility information

Building management information

Floor plans

Hardware and software inventories

Key forms

Physical Site Preparedness

Physical site preparedness can also aid in reducing the severity of a disruption. For example, having working flashlights handy in a power outage can make the difference between being able to shut down a system gracefully and a hard crash. Having a reliable means of communication among the members of the technology staff is also key. This means keeping charged cell phones and/or walkie-talkies available.

Vendor Plans

What happens if a key vendor has a problem that affects your operations? At first blush this may seem beyond your control, but in fact, there are steps that you can take to protect your firm against this type of problem.

One criterion for selecting key vendors is that they have disaster recovery plans of their own. Also, one component of your overall backup plan is to include alternate providers that can be used in the specific event of a disruption to the operations of key vendor services (e.g., payroll system, litigation support service providers and ISP).

Training

Training falls into two categories. One is for users. Those who are better trained are more self-reliant, so that in a disruption the more likely they will be to get their work done from home or a backup location.

The second training category is for the technology staff. The better trained they are to deal with a disruption, the more likely they will be to solve problems. This training should include the content of the firm’s business continuation plan, the technology and procedural issues involved and remote access, among other things. In addition, cross training among the staff should also be included.

Common-Sense Business Planning

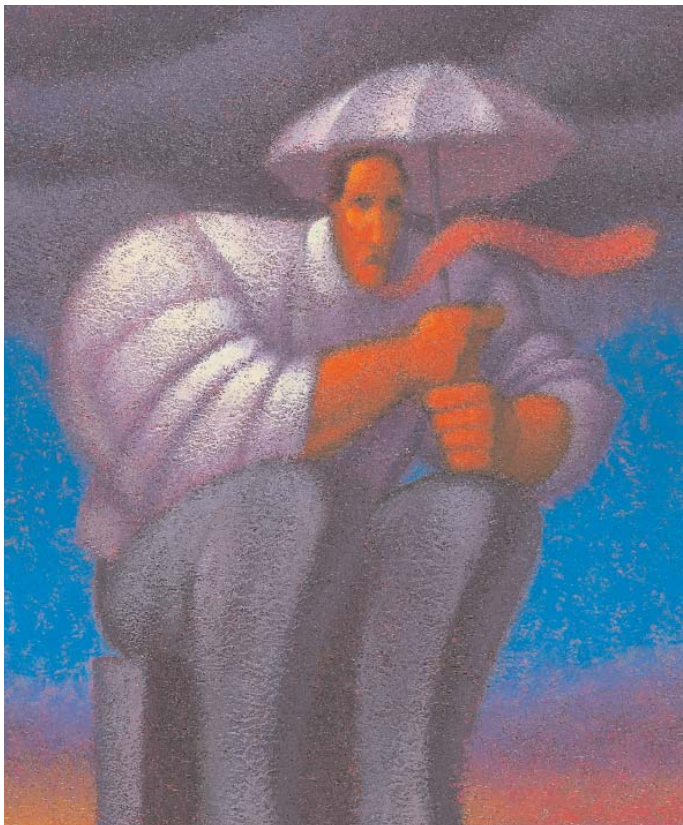
Make sure that you have emergency purchasing procedures and access to adequate funds in the event of a disruption. Some firms have implemented revised purchase approval process for emergencies.

Testing

Even the best business continuation plan, if not periodically tested and tweaked, is likely to present unexpected and perhaps unpleasant challenges when the time comes to use it. To minimize the length of a disruption you should do periodic testing. Too many firms have learned the hard way that they could have substantially reduced their outage if testing and improving the plan had taken place.

It's Never Too Soon to Start Preparing

We hope the information in this article will help you avoid disruptions whenever possible and minimize their length and severity if they do occur. And remember, the time to start preparing is *now*. It's never too early!



Using the Web in Times of Crisis

by Maureen Reidy Leuenberger of Hubbard One

Communication is the backbone of business continuity planning, and many forward-thinking firms are carefully putting cost-effective infrastructures in place to use secure websites and extranets to supplement traditional channels of communication during times of crisis. The Web's natural strength lies in its reliability and availability as a communication channel. By extending the capabilities of Web-based content management tools, law firms are now deploying and managing content in business continuity Web applications at any time from any location where there is an Internet connection.

Case Studies

Hale and Dorr developed a rapidly deployable secure staff extranet system to conduct online roll call in times of crisis, supplementing or replacing traditional check-in processes. Similar extranets can also include contact and alternate workplace facility information, as well as a moderated Q&A component. Additionally, integration of business continuity extranets with HR systems (such as PeopleSoft) enables fast cross-referencing against official staff lists.

Willkie Farr & Gallagher put the technology in place to instantly replace its homepage with an alternate emergency homepage rich with information for clients, the media and public. Other firms allow for a link from their homepage to a new page with crisis-related information or for activation of a popup box with emergency information.

The "Crisis Management Team" at Paul, Weiss, Rifkind, Wharton & Garrison, which is composed of partners and management staff, has access to the company's business continuity plans and firm contact information through a secure management extranet that is always accessible. Availability of such a system is as important as the system itself. A best-in-class, managed systems-hosting environment, as opposed to in-house hosting, dramatically increases availability and accessibility.

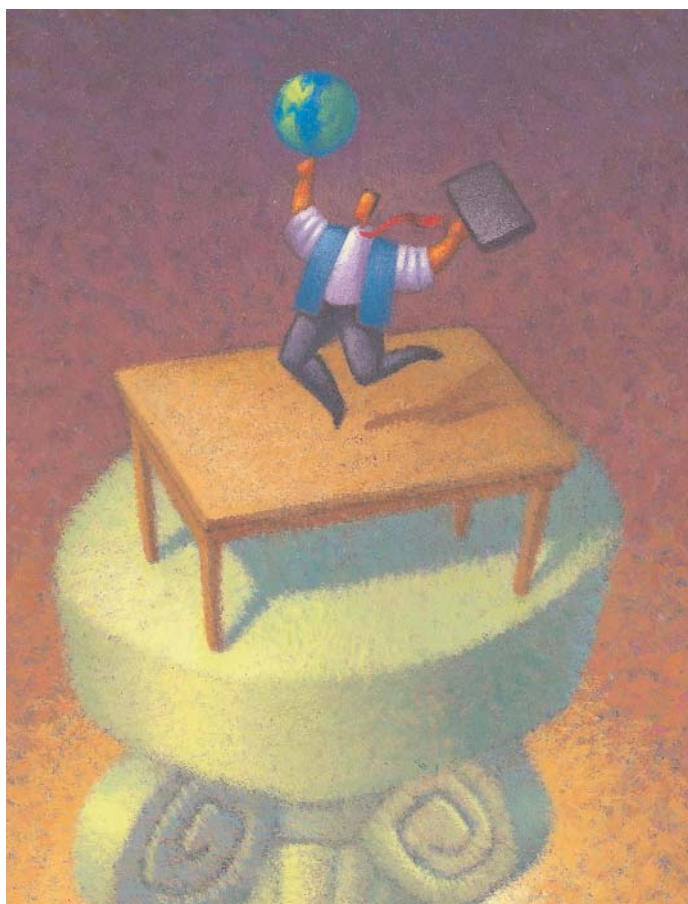
The Bottom Line

Business continuity applications such as staff extranets, homepage failover applications and management extranets are increasingly becoming some of the most highly visible, yet cost-effective, components of successful business continuity communication plans.

Disaster Recovery Planning

Being Proactive Is Key!

by Craig A. Parrish of SSD, Inc.



In the aftermath of the catastrophic September 11 terrorist attack and, more recently, the massive Northeast power grid outage, many law firms are focusing greater attention on disaster recovery and business continuity planning—not only to prepare themselves for a big disaster but also for lesser ones within regional offices that could detrimentally impact personnel safety and revenue. In preparing for disaster, it is important to focus on three basic, yet vital, issues: life safety, critical systems recovery and relocation planning.

Life Safety

Any disaster recovery plan must start with the guaranteed safety of the employees, which includes the issues of evacuation, accountability and ongoing communications. It is important to be aware of these three things: one, the building and its location are vital in the evacuation of personnel; two, each individual must be responsible for himself or herself; and three, it's best not to assume that a top-down accountability process will work effectively.

Evacuation

It's essential to have an organized, practiced process that employees know and will follow in an evacuation; you do not want people in time of crisis having to stop to make decisions, for this almost surely leads to greater confusion and critical delays. Advanced preparation is critical—firms that instituted and practiced effective evacuation processes following the 1993 bombing of the World Trade Center had better success saving employee lives during the 2001 terrorist attack.

Proper signage is vital. While building codes require lighted exit signs to direct personnel to the fire stairs, many signs may not give proper direction or may not light at all. Check your signage. Exit signs should be clearly visible and appropriately direct personnel to designated fire stairs. They should also be lit normally with power on, and they should also be lit during any test to ensure they are in good working order.

Based on the layout of the building and fire stairs, employees should be assigned to volunteer safety coordinators who are educated and equipped for the evacuation process. Personnel are also given special gear for evacuation which, at a minimum, includes some sort of a powerful keychain light (e.g., Photon light with a 10-year battery), a safety mask (3M makes the ones that were used during SARS scares) and a whistle.

Accountability

A proven method of accountability is a bottom-up process that starts with individual employees. An external voicemail system process can be established that allows employees to call an 800 number and leave a message that they are safe and how to contact them. Voicemail systems used for accountability are typically located outside of the regional area of the office that you're protecting. Firms are either creating additional capacity within internal telecommunications systems for this capability or contracting with third-party

voicemail providers such as VoiceComm. Note that these voicemail systems require significant incoming line capacity to ensure that callers do not get a busy signal. The systems are generally set up with a company greeting, office and floor selections, even a section delineation by floor. The setup directly matches the safety coordinator personnel assignment for evacuation. Messages can easily and quickly be retrieved, and firms can then focus attention on locating the minority of missing individuals who have not left an accountability message.

Medical Response

Many firms have established medical response programs in response to specific internal medical issues or health problems associated with attorneys or staff members. At the heart of such a program are medical responders and a quality medical training program. Many volunteer medical responders have had previous training at work, in Boy/Girl Scout or YMCA/YWCA programs or in lifeguard training, nursing, premed or paramedic programs.

Firms with multiple offices in many regional areas will select national training groups to facilitate a program that is consistent from office to office. The American Red Cross, which has strong training programs for general first aid, CPR/AED and oxygen administration, is a great resource. In addition to the programs, they provide training materials and instruction sheets to make available to employees. Using a nationally recognized training group limits the liability for the firm with respect to first aid assistance administered by firm personnel. An extra benefit is that a strong medical response process can often lead to a health and wellness program that promotes a safer and healthier workplace.

Medical response typically starts with a call to the receptionist reporting a medical emergency. All medical responders are summoned to the location where the injured party is located. The first medical responder on the scene administers first aid; the second assists in first aid administration; and the third responder facilitates communication with emergency personnel and provides the necessary medical equipment. When professional EMT workers arrive they take over the administration of care to the injured party.

Critical Systems Recovery

While many firms understand the value of life safety, it is often more difficult for them to determine the value of critical systems recovery and business risk. A strong business risk analysis clearly identifies the risk potential and the impact that a given disaster scenario would have on the firm's business and revenue. It is this revenue impact that will clearly

influence attorney and committee support to move forward with the systems recovery planning process. Consider the following disaster and revenue impact from two nonlife-threatening disaster scenarios.

Scenario One: Virus Infection

A firm is infected with a virus. Of 220 workstations deployed in its regional office, 120 require immediate replacement from the damage caused by the virus. It takes the full attention of the firm's IT group to purge the virus from the network and three and a half weeks of outside support from their integrator. The firm suffers two days of downtime.

Cause

The firm suffered a virus infection from a known virus. The infection could have been prevented if the firm's virus software definition files had been up-to-date. The update was commercially available 18 months prior to the infection.

Impact

The firm produces \$250,000 in daily revenue. With two days of downtime, the revenue impact was \$500,000. The cost for the replacement computer workstations was \$126,000. The cost of outside integrator support was \$31,000. The direct allocated cost of IT department support was \$17,200. The total cost impact of the disaster was \$674,200.

Scenario Two: Local Power Outage

There is a loss of power to a firm's building in which its main office is located. The outage lasts for 14½ hours. The firm has a point-to-point wide area network (WAN) with consolidated Internet, e-mail access and interoffice data communications; and all communications originate from the main office in support of its satellite offices. The firm has 20 minutes of battery backup time before the servers shut down. The office telephone system is part of a multitenant system run by the building. The building has two hours of UPS battery support before all communications for the main office become unavailable.

Cause

The power outage was caused by a problem in the connections to the building by the local utility company. The firm lost all Internet access, all incoming e-mail access, all data communications between offices and all voice communications within the main office.

Impact

The firm produces \$320,000 in daily revenue from this office. The cost for operations without associated revenues is \$105,000. The measurable cost impact was \$425,000. The

impact to client case activity from the complete loss of e-mail and Internet access for the day: immeasurable.

It is eye opening to review these disaster scenarios. The cost for prevention and deployment of systems that would have prevented or significantly lessened the financial exposure to the firms experiencing these events is only a small fraction of the impact of the disaster (less than one percent in the first scenario, less than five percent in the second). Presented with the risk potential, cost for prevention and impact to operations, firm partners would surely have chosen a more proactive approach to prepare for such vulnerabilities.

Experience has taught us that while many firms plan for the most catastrophic disaster (a complete and permanent loss of their primary site); the reality is that there are many basic disaster scenarios that require different kinds of recovery responses. These scenarios include:

- Complete and permanent loss of primary site*
- Loss of data center (fire, HVAC)*
- Indefinite loss of building access with risk escalation (fire, anthrax)*
- Short-term predictable loss of building access (snow emergency)*
- Telecommunications/communications service loss (e.g., cables cut)*
- Power outage lasting more than one hour (transformer)*
- Internet outages (e-mail and user access)*
- Network infrastructure outage*
- Network infection/security breach*
- Application information store corruption*
- Server outage*

Structuring a direct critical systems recovery response to each of the scenarios, determining current recovery methods and time frames for setting appropriate attorney expectations and exploring practical system upgrades using expanded recovery methods are prudent measures any firm should take.

Telecommunications Redirection

Following the events of 9/11, many Bell operating companies and long-distance carriers established programs to allow for the redirection of incoming phone calls to firms. The firm would have the ability to create detailed redirection lists and forwarding instructions for incoming calls for both central office main number calls and direct inward dial (DID) calls. Calls can be redirected on a percentage basis from one office to other regional offices (e.g., directing 33 percent of the calls

from New York to Chicago, 33 percent of the calls from New York to Atlanta, 33 percent of the calls from New York to San Francisco). Planning is required if calls are to be redirected to regional offices to ensure that the capacity of the regional offices' systems can handle the traffic and that associated voicemail systems are configured for messages that would be left by callers. An alternative for single-site firms or firms lacking the telecommunication capacity is to facilitate service through a third-party provider for virtual telecommunications services such as VirtualPBX.

Services include:

- Telecommunication system locations outside of the firm's regional office area*
- Multiple incoming lines*
- The ability to have calls directed to their telephone system, which would then automatically forward the call to cell phones or home phones for the attorneys*
- Voicemail for the caller to leave a message that can be retrieved at a later time*

Critical Relocation

Relocation planning involves the selection of a temporary or permanent recovery site and the expedited buildout and relocation of personnel and systems to that site, assuming that the primary building location is unavailable.

If a firm experiences a situation which necessitates immediate relocation, having a relationship with a real estate business management or development group with ready access to facilities in the same geographical area is wise. Such a relationship significantly helps the firm identify and lock in space if required without competing with other companies in the same position.

Law firms typically work with architects, engineers and design groups anywhere from six months to two years prior to a relocation of a facility. Following a disaster, these design cycles must be significantly shortened in order to reduce business and revenue impact to the firm. If a firm establishes requirements for the building and tenant space and preselects contractors that would be available to help facilitate this process, the relocation can be expedited.

Desirable building resources for new and current space have been expanded over the past few years. Following are some examples of which you should be aware:

Construction

- Following the World Trade Center terrorist attack, it is clear that insulation for structural steel and additional*

reinforcement of building cores, especially around fire exit stairways, will be included in new construction code changes. Also, fire stairs will be expanded to facilitate full rather than, as in the past, partial evacuation.

It is best to vertically stack both electrical and signal cable riser closets to prevent service routing problems through the floors of the space. Multiple risers on different sides of the space are also preferred. The closets should either be cooled or well ventilated.

There should be multiple entrances/exits to the building, and they should be easily accessible for evacuation but properly secured, to prevent a physical security problem.

Main sprinkler feeds should align with hallway space and run outside of critical core area space (i.e., computer room, IS area, copy center, records) and offices.

Cable trough/trays separated for electrical and signal cable systems that would core closets and traverse the hallway areas of the space would be preferred as a building standard. A trough between the computer room and the signal riser closet is also preferred.

The building grounding should be reviewed prior to construction. A true, earth ground separated from steel and separated from the grounding of floor electrical riser equipment is preferred.

Services

The building space should be designed for closed office tenant space with respect to heating, ventilating and air conditioning (HVAC) services.

It is best to have well separated, multiple feeds to the building for water, drain, power and signal systems.

There should be building management tie-ins for each of your floors for building and tenant security and multizoned floor fire alarm systems.

All building exit signs should be LED to eliminate bulb-replacement maintenance.

Signal feeds from communication carriers should be fiber. The local Bell operating company feed ties you back to a Sonnet Ring or major service feed if possible. This will enhance the type of services and service options to which you have access, and it will allow for better service level agreements and faster service reconfiguration and response.

The building electrical system should separate lighting and mechanical services from standard services.

The tenant electrical system should also separate standard electrical services into standard convenience and computer services.

Signal riser closets should include multiple fiber connections between the tenant space and the base building services room(s).

Review of HVAC, emergency power diesel generator, water pump and other building service systems should be done with design focus on redundancy, efficiency and serviceability.

Riser space and termination consideration for cable TV, video teleconferencing, security and high-speed communication feeds is also preferred.

If the need for relocation arises, the time it takes will be significantly reduced by having a complete list both of current building and tenant requirements and of trusted contractors that would be able to facilitate buildout and relocation. Organized planning will create office-to-office consistency in design and allow for greater consistency in firm disaster recovery planning over time.

Conclusion

Proper disaster recovery preparedness will mitigate risk, empower employees and improve current business processes. Many firms are pleasantly surprised by the efficiencies gained through the effort. Remember the adage “Be Prepared” when embarking on the process of structuring a disaster recovery and business continuity program. Proactive process and careful preparation will go a long way in averting a disaster or minimizing the impact if one occurs.

Online Backup and Recovery

Overcoming the Trials of Data Protection

by Bob Cramer of LiveVault Corporation



It's Wednesday evening and you're paged by your law firm's lead partner as you're driving home. It seems someone accidentally downloaded a computer virus at the office, and all systems are down. Most importantly, the partner and his staff just lost a day's worth of work for a trial that begins tomorrow. As the only IT person on staff you normally back up your firm's data each night to tape, but usually at midnight when the office is empty. You're confident you can have the network up and running by the next morning—but on Thursday morning you'll only have, at best, Tuesday night's data.

For most small and medium-sized businesses (SMBs) formulating business continuity plans, the first concern is typically how fast they can get their business up and running again. While this is a critical concern, it's only half of the recovery equation. The other part of a recovery plan needs to focus on the amount of data the organization can afford to lose.

A law firm's most valuable asset is its data. The data might be thousands of legal files or years of billing information—but even the loss of one file can put your firm in jeopardy. In the past, SMBs like law firms or insurance agencies have had only one option for data protection: nightly tape backup. But sadly, industry analysts estimate that more than 50 percent of tape backups fail to restore properly. As a result, these businesses are at considerable risk of losing their data, a loss that can cause irreparable harm to business operations.

Most SMBs have Windows servers at the center of their technology infrastructure and typically are running Microsoft's Exchange Server, Microsoft SQL Server-based applications, Oracle-based applications or Web applications. Without any of these, their businesses would stop functioning in very short order. Yet many firms have probably never tested their backups or tried to recover their business data and have not asked all the associated questions:

Can I recover all of my most recent critical data using my current methods?

Where are my backup files? Are they offsite?

Who has custody of the backup files?

When were the applications and databases last backed up?

Can I recover my data quickly enough?

Does the backup method work?

Negative answers to all or even some of these questions add up to the same ultimate risk: business continuity failure.

During the last several years, new enterprise-quality data protection technologies have become available for small and medium-sized businesses. Until recently, backup and recovery technologies that operate on a continuous rather than nightly basis, common at larger enterprises, were seldom considered by SMBs due to the expense. Similarly, establishing business continuity metrics such as Recovery Time Objective (RTO: the amount of time a business can be down, by process or

application) and Recovery Point Objective (RPO: the amount of data a business can afford to lose) have been integral in large enterprise business continuity planning for many years and are just now becoming relevant for SMBs. With new technologies like broadband and online backup and recovery making more affordable disaster recovery solutions available to SMBs, the critical questions now are:

What technologies should we consider for disaster recovery?

What level of protection do we need?

At what cost?

Business Continuity Metrics

SMBs need to determine a balance between the level of business risk they can tolerate and the cost of perfect security. Initially, all businesses would say they can't afford to lose any data or tolerate any downtime. But protection on that scale is probably cost-prohibitive and overzealous. It's unlikely that in a business of any size all applications are equally mission-critical and all systems equally vital. That's when metrics like RTO and RPO enter the discussion.

International Data Corporation research has determined that 98 percent of all companies are adversely affected by unscheduled downtime. This speaks directly to the need for RTO to guide your law firm when disaster strikes. Having tested and proven RTO metrics will give you confidence in how quickly you can recover your most important systems.

In addition, Gartner Group research found that 93 percent of organizations that have experienced a significant data loss are out of business within five years. This research confirms the need for RPO: in the event of a disaster, once your law firm's systems are back online, your RPO standards help you keep data loss to a minimum.

Business continuity plans start by determining the RTO and RPO for a particular firm's applications. The relative importance of RTO and RPO is different for every organization. For example, an e-commerce website may tolerate a higher RPO than RTO because, while the business cannot afford to be offline, orders that end up backlogged may not affect the customer experience as negatively. A law firm, however, would likely have close to zero RTO and RPO, for not only does it need to be up and running quickly; but since the large majority of law firms store most of their files electronically, attorneys need immediate access to their up-to-date files to continue serving and billing their clients.

While every law firm has near-zero RTO and RPO expectations, most don't have the proper solutions in place to

meet these expectations, because till now they weren't able to afford this level of protection. The ability to minimize both the recovery time and amount of data lost can only be achieved with a solution that addresses every aspect of the backup and recovery process. To fully understand how SMBs can meet both RTO and RPO goals, let's first examine how the majority of data is protected today.

The Importance of Data Protection

Four primary assets are needed to effectively operate an information system—facilities, hardware, network and data. In the unfortunate event of a disaster, hardware and networks can be replaced, and facilities can be moved to a new location. In fact, with the exception of data, virtually every company system asset can be replaced.

Every organization has a core set of data upon which it depends. Whether it's payroll information, customer records, valuable research, financial records, e-mail files—all corporate data is valuable and thus is vulnerable to loss or irreparable damage. Data loss can result from any number of factors:

Human error

Operating system or application software bugs

Hardware failure

Fire, smoke or water damage

Power outages

Employee theft or fraud

Manmade disasters such as sabotage, hacking or viruses

Natural disasters such as earthquakes or hurricanes

Any one of these factors can cause data loss, and the results can be catastrophic. It can result in the loss of irreplaceable information or files that may take hundreds of hours and thousands of dollars to recreate. For today's organizations, the loss of their most important corporate asset can have an incredibly negative impact in real dollars, lost opportunity, customer dissatisfaction, shareholder insecurities and overall corporate image. Regardless of the cause, data disruption and loss pose a significant risk for any business.

So what should companies do to preserve their data? Law firms and other SMBs must implement a solution that incorporates the following four components:

Continuous backup

Offsite vaulting

Immediate recovery

Guaranteed recovery

Requirement #1: Continuous Backup

SMBs are exposing themselves to extreme risk when it comes to backing up their data. Only half of the SMBs in the U.S. perform some form of data backup, and surveys find that these businesses do not always do an adequate job. Because they have limited or no IT staff to handle backup, they perform bulk server backup sporadically, use traditional tape for backup and typically perform the task after business has closed for the day. That means that if a virus, fire, power outage, natural disaster or human error results in the need to restore data, the most recent data most law firms can expect to recover is the previous night's data.

Requirement #2: Automatic Offsite Storage

Even if your law firm is rigorous about backup, and you're sure that you have at least last night's data available to recover if you need it, are you equally rigorous about ensuring that the tape is safely stored in a secure offsite location? Perhaps you do invest in scheduling the time to backup and remove tapes physically and arrange for pickups by a third-party to transport your tapes to a vault located outside your immediate radius. But more likely your firm does not currently make these investments, and this fact exposes you to serious risk.

Requirement #3: Immediate Recovery

Recovery is the process of restoring operations and specifically, data, after an outage or disaster. Alarmingly, even in best-of-class IT shops an estimated 20 percent of all backups fail to fully recover. The primary causes of recovery failure are human error, improper configuration, tape media failure and mishandling. It's an obvious point, but often overlooked: being able to immediately recover data is critical to ensuring business continuity.

Requirement #4: The Guarantee

There are very few, if any, guarantees in the IT world, especially when considering disaster recovery preparedness. Backup and recovery software vendors will have RTO and RPO ranges within their service level agreements; however, none will provide an absolute guarantee, for there are too many elements outside of their control, like tape quality or the competence of the internal IT staff.

Online Backup and Recovery Services

Now that you have learned about the requirements for meeting stringent RTO and RPO standards, specifically how do online backup and recovery services help meet these objectives?

Online backup and recovery services are managed services. This means that the entire process is managed outside of your

law firm by an expert third-party using the provider's hardware and staff. Managed service providers can do this cost-effectively because of their expertise in leveraging advances in data replication and security technologies, combined with reduced bandwidth and disk costs. Secondly, online backup and recovery solutions offer data protection services remotely—so your business data is automatically and instantly offsite, almost as soon as you create it. Most importantly, online backup and recovery solutions map directly to the requirements outlined above that highly productive law firms require: continuous backup, offsite vaulting, immediate recovery, guaranteed recovery.

Continuous Backup. Thanks to secure Internet technology and advances in creating greater bandwidth for SMBs, online backup can provide continuous backup—and therefore protection—of your critical data assets. Continuous backup allows data to be captured as it is changed—essentially in realtime—so that any changes in a file are captured and protected immediately. Online backup and recovery services offer these advantages:

Enterprise-class data protection. With online backup, law firms of any size have access to the same high level of data protection the large organizations enjoy. Unlike tape-based backup where information is backed up every 24 hours or even less frequently, online backup and recovery options back up information on a continuous basis. Continuous backup eliminates the “window of vulnerability” inherent in tape-based backup. Not only is data up-to-date, but in the event of a disaster, organizations can immediately recover and restore lost data with the click of a mouse, without having to worry about retrieving off-site tapes and manually initiating the process.

No IT maintenance. There are no tapes to switch out or bring offsite. Once the agent is installed on a server, online backup and recovery works on autopilot. With continuous backup, all data changes are automatically transmitted via a secure Internet connection to an offsite location. Backup administrators don't need to perform special functions to keep the service running. Online backup and recovery takes away the burden of backup and lets IT professionals focus on IT concerns that are strategic to the business.

Reliability. Because server data is automatically backed up, human intervention is eliminated, thus limiting the potential for human error. In the rare case that the connection to the offsite vault is disrupted, a fully managed service provider will be able to notify its customers

of the outage, taking proactive steps to remedy the problem.

Automatic Offsite Storage. Online backup and recovery services automatically back up your data to an offsite, secure storage facility. By transmitting the data via the Internet, physical damage to tapes is avoided entirely, and the data is immediately available for system recovery. Without automatic offsite storage, you never know until it's too late whether or not the data is stored in a safe environment. But luckily, with online backup and recovery services, the availability and security of your data is assured.

Specifically, these services provide:

Safe and accessible data vaulting. *Online backup solutions ensure that data is never in an unsafe environment and is always accessible. These solutions address concerns over improper storage by protecting data offsite in a secure data center.*

Simple and low-risk data removal. *Data is no longer at risk of not being moved from your office premises or of being mislaid during the removal process. Tape damage or mishandling as well as transportation issues are completely eliminated.*

Standardization. *With online backup and recovery, IT administrators needn't worry about whether backup at remote locations is being done properly; the process is automatic.*

Immediate Recovery. Online backup and recovery services provide the only system by which data is available for immediate recovery. Even the most diligent IT organizations that transport their data to secure offsite storage facilities need time to retrieve the data and initiate the recovery procedure. By using online services, data is available as quickly as the user can access the Web. Once the user is logged into the service, the recovery process can begin.

Recovery using online backup and recovery also provides:

Convenience. *Even single files are retrievable with online backup. With tape backup, you wouldn't even consider trying to recover only a single file because the time and inconvenience of retrieving the tape, searching for a particular version and attempting a restore is too onerous. But online backup offers a point-and-click alternative that makes it easy to restore in seconds even that single client presentation your senior partner accidentally deleted.*

Ease of manageability. *Some online backup and recovery providers allow customers to manage their data protection process through a personalized Web management interface, so firms can view the status of their data and initiate a recovery from anywhere—through any Web browser. While the service provider assumes responsibility and automates back-end functions, users retain overall control of their data protection by creating customized backup policies, checking status and initiating restore operations whenever needed.*

Cost-effectiveness. *With online backup and recovery, users don't need to pay for tapes, software, hardware, ongoing maintenance and offsite tape storage contracts. The service is billed as a recurring—typically fixed—fee. Because the service is much more reliable than tape-based backup, should a disaster occur, users do not need to pay for data retrieval or spend employee hours recreating data. The data is easily restored online.*

A Guarantee. Online backup and recovery services, unlike typical IT departments dependent on tape for backup, are able to provide the luxury of a guarantee. Because the entire process is managed by experts at the service provider, and the technical components of the service are fully automated, online backup and recovery services know their ability to restore an organization's data. When evaluating any backup and recovery solution provider, make sure to ask if they guarantee recovery.

Summary

Online backup and recovery services provide the easiest and most cost-effective way that, in the event of a disaster, law firms can be sure that they're able to get up and running quickly without any data loss. Online services have made it easy for SMBs like law firms to set realistic and aggressive RTO and RPO standards for business continuity—an important step in protecting a business from disaster. Maximizing RTO and RPO requires four major elements that only online backup and recovery services can provide in a cost-effective manner for law firms. But most importantly, these services are the only way to guarantee that your firm will still be able to operate in the event of a disaster.

When it comes to disaster recovery planning, do you want your law firm up and running quickly, but operating with data that's a week or even a day old? With online backup and recovery solutions, you don't have to make that tradeoff—you can have it all.