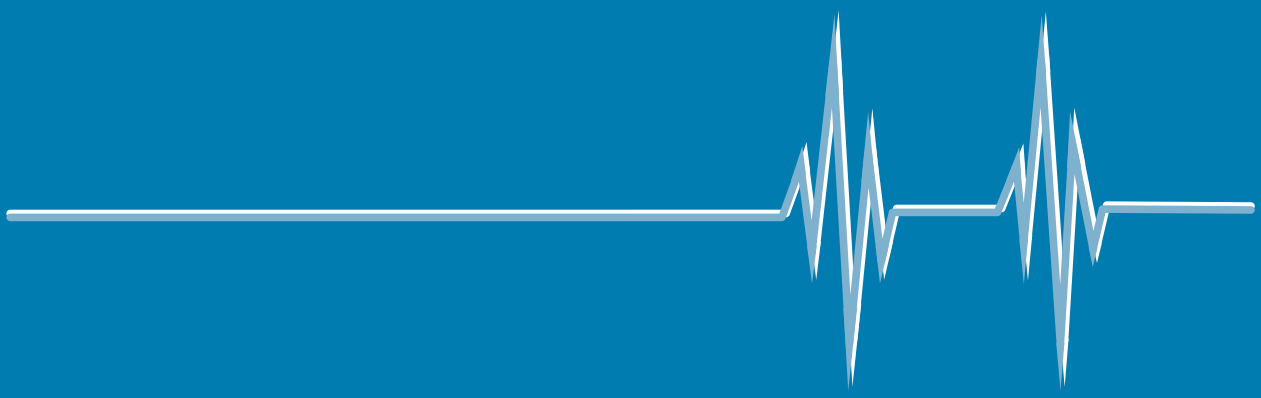
Executive Focus White Paper

How Digital Document Management Streamlines Business Continuity Planning



Learn more inside:

- What is a "disaster"?
- How does disaster recovery planning differ from business continuity planning?
- How do I develop a business continuity plan?
- What role can digital document management play in my business continuity plan?

How Digital Document Management Streamlines Business Continuity Planning

A Laserfiche® Executive Focus White Paper

Introduction

During the 1990s, it was common for organizations to require a three-day window to recover from a disaster and return to normal operations. By 2001, a one-day delay was considered acceptable, but **today recovery time objectives (RTOs) are between zero and four hours.**

What's changed?

Today, organizations have more than just a server to recover. Now, there are several platforms that must be restored, ranging from mainframes and distributed processors to servers, PCs and telecommunications systems. More complicated data recovery solutions, such as data replication, mirroring, clustering and tiered storage, are required to help organizations cope with the unexpected and rapidly resume operations.

Also, organizations have begun to realize the impact of disaster. In 2004, ESG, a consultancy group focused on storage and information management, found that if applications were up and running, and if critical data was recovered within four hours of outage or system failure, odds were favorable the business impact would be manageable. For organizations like online merchants or online brokerage firms, this recovery window is even shorter, as the value of data has increased and corporate governance requirements have mounted. Depending on the organization and industry, the time to get critical applications up and running after an outage has decreased from hours to minutes or even near zero.

For organizations that rely on their IT systems as a revenue generator, not solely as a record keeper, the importance of guaranteeing uptime is crucial. For these IT systems, value is attached on a minute-by-minute basis. While losing organizational information is disastrous, losing transactional information—and its associated revenue—can be catastrophic. With more and more small- and medium-sized businesses relying on transactional data from Web sales, POS systems, e-mail and fax archives and VOIP systems, losing access or connectivity through downtime means an extensive loss of revenue. Protecting your organization from downtime is crucial to minimizing its impact.

Business continuity planning is the solution to mitigating the impact of a disaster, no matter its source. Industry estimates show that **40% of organizations without business continuity and recovery plans will go out of business within a few years of a major disaster.** In fact, the Institute for Business and Home Safety, an insurance industry trade group, estimated that **25% of businesses that close during a disaster will not re-open.**

This white paper discusses how a digital document management solution can help your organization develop and implement a comprehensive business continuity plan. Learn what disasters are and how disaster recovery and business continuity planning work in tandem to help your organization react more effectively, and discover strategies for developing a plan of your own.

Defining "Disaster"

Defining what a disaster actually is has become crucial as organizations shift their perception of disaster. When you think of a "disaster," natural disasters like floods, fires or earthquakes immediately spring to mind. But consider:

- **A pandemic.** Recent projections show that an avian flu pandemic could potentially infect millions of people over an undefined period of time. In fact, the Congressional Budget Office estimates that in an avian flu pandemic, 30% of employees would become ill, missing an average of three weeks of work. Of those who become ill, 2.5% will die. If a large portion of your workforce is incapacitated, do you have contingency plans in place to replace missing employees?
- **A transportation strike or public transit failure.** If there is a disruption to the public transit system, whether by strike, infrastructure failure or natural disaster, it is likely that many of your employees will be physically unable to travel to work. Do you have plans for virtual offices or off-site accessibility? What about alternative transportation plans for your employees?
- **A bombing.** After the Oklahoma City bombing, 40 square blocks were barricaded off for weeks. Do you have a plan in place in case your office space is destroyed or otherwise uninhabitable?

It isn't just catastrophic disasters that you need to plan for, although they do get the most attention. Even minor incidents like brownouts or freezing rain can cause network outages ranging from minutes to days, and in these cases, rapid recovery is crucial to maintaining productivity and restoring revenue generation.

Shift Your Perception

Disasters A to Z

Acts of war, arson, blackouts, blizzards, bomb threats, bribery, bridge collapse, brush fires, chemical accidents, civil disobedience, communications failure, cyber attack, disease, disgruntled employees, earthquakes, embezzlement, explosion, fires, floods, hardware crash, high winds, hostage situations, hurricanes, ice storms, interruption of public infrastructure services, kidnapping, labor disputes, lightning, military operations, mudslides, network failure, plane crashes, railroad accidents, sabotage, SARS, server failure, snow storms, software failure, terrorism, theft of data, thunderstorms, tornados, transportation strike, vandalism, viruses, water damage.

...what else can you think of ?

A reasonable definition of a "disaster," according to *Disaster Recovery Planning: Preparing for the Unthinkable,* is "the unplanned interruption of normal business processes resulting from the interruption of the IT infrastructure components used to support them."[1] This definition includes not only networks, hardware and software, but also data itself.

A 2007 IDG Research study showed that **92% of respondents have encountered at least one disruption to their business systems.** While high-profile events like hurricanes, earthquakes and terrorism get attention, they serve as distractions from the real threats: **65% report disruption from power failure, 65% from network outage and 55% from hardware failure.** Focusing on natural disasters and terrorism diverts attention from the realities of today's business environment and the deteriorating state of IT infrastructure.

It is clear that the definition of "disaster" must be expanded beyond just forces of nature to include everything that can impact your organization's operations, from employee absenteeism caused by an epidemic to corporate theft, vandalism and long-term unavailability of basic services. With proper planning, your organization will react with equal agility to something as commonplace as a server crash or something as seemingly unimaginable as an asteroid impact.

Lessons from Past Disasters

2005's Hurricane Katrina once again brought home the importance of comprehensive disaster recovery planning. With a cost of over $200 billion—with the greatest losses from disruption to businesses faced with damaged facilities, displaced employees and business interruption—Katrina caused organizations to face the question of whether they are truly prepared to recover quickly and continue operating after a disaster.

There was a surge in disaster recovery and preparedness planning after September 11, when organizations were forced to consider how they would continue operations if their offices were uninhabitable for not just weeks, but months or years. But these plans began to gather dust as executives were lulled into complacency. Months, then years, went by without updating or testing disaster recovery plans.

When the Northeastern Blackout of 2003 hit, organizations were left with out-of-date and inadequate recovery plans. This massive power outage occurred throughout parts of the northeastern and midwestern United States, and Ontario, Canada, on August 14, 2003, affecting approximately one-third of the population of Canada (10 million people in Ontario) and one-seventh of the population of the United States (40 million people in eight states). **Outage-related financial losses were estimated at $6 billion.**

The Northeastern Blackout was a huge catalyst in the changing perception of what disaster recovery planning actually means. As a result of the September 11 attacks, the US Securities and Exchange Commission (SEC) and other government agencies had recommended that all Wall Street firms move their backup facilities from 50 miles outside of New York City to 125 miles, as well as put them on a separate power grid. The establishment of "Wall Street West" in the Poconos allowed real-time mirroring of IT systems

---

[1] Retrieved August 28, 2007 from
http://www.informit.com/articles/article.aspx?p=30944&seqNum=3&rl=1

and, during the blackout, enabled financial markets—as well as many businesses—to continue operations by "failing over" to their mirrored backups. Businesses that hadn't developed comprehensive business continuity plans, however, faced crippled operations and a significant loss of revenue.

The situation hasn't improved since. In a recent study conducted by the Association for Financial Professionals, **only 37% of those surveyed feel their organization could handle a Katrina-like disaster.** Most telling, only 24% had tested their business continuity plans as a direct result of the hurricane, and 50% had no plans to do so.

Specific Lessons Learned From Past Disasters

- Consider an off-site real-time mirrored failover location on a separate power grid, so that you can continue operations in the event of a power outage or natural disaster localized to your immediate area.
- Assign back-up roles in case key players are unavailable or missing.
- Plan for all possible communication issues, including use of satellite phones, hotlines and Web alerts.
- Establish accessible spending accounts for employees, make standing lodging arrangements near your recovery site and account for other logistics, like mail delivery and payroll.
- Plan for extended recoveries, in case business is displaced longer than expected.
- Keep your organization's documentation, scripts and business continuity planning handbook up to date.
- Provide an alternative method of accessing your data and documents.
- Be sure all vendor contracts are complete and up-to-date, including those with providers of media storage, insurance and fuel.
- Plan for business continuity, because no one else will do it for you.

Disaster Recovery and Business Continuity Planning: Mutually Exclusive, or Better Together?

The terms "disaster recovery planning" and "business continuity planning" are often used interchangeably, but they are two different concepts that work together as complementary components of a business's overall recovery and continuity planning.

Disaster recovery planning (DRP) is chiefly concerned with the recovery of systems and infrastructure components. By definition, it is limited in scope to a set of defined IT systems and infrastructure, with the ultimate goal of complete recovery within a defined timeframe and with a minimum of data loss. Because of the heavy emphasis on IT infrastructure, it may exclude non-IT business units such as accounting, marketing and sales, except in terms of software applications used by these departments. One issue with disaster recovery planning is that, because of the IT focus, incorrect assumptions may be made or subtleties or dependencies that are not hardware or application dependent—such as document management, document retention and security—may be missed.

Business continuity planning (**BCP**) is an attempt to blend the IT emphasis of disaster recovery planning with a larger-scope determination of which business components and functions must be prevented from interruption or, if interrupted, recovered immediately. It is an iterative process designed to identify these mission-critical functions and enact the policies, processes, plans and procedures that ensure their continuation if an unexpected event were to occur. The exact functions covered by BCP vary by industry and may include processes that are not necessarily software applications, but also infrastructure (office space), supplies (marketing materials and forms) and human resources. BCP is also governed by industry-standard regulations, such as the Sarbanes-Oxley Act, HIPAA and FDIC/SEC rules and regulations, as well as "quasi-regulations"—industry standards and best practices that should also be followed—such as FEMA 141, which covers disaster recovery planning for business and industry; ISO 15489, which governs records management; and NFPA 232, which concerns the physical protection and storage of documents.

Basically, **your organization can have a working disaster recovery plan without a working business continuity plan, but not vice versa**. For organizations that have neither, the best move is to start by designing a plan that is a blend of both. For organizations that have already developed a disaster recovery plan, that knowledge can be leveraged into the creation of a business continuity plan.

The scale, cost and impact of a business continuity plan are enterprise-level and must be managed by a C-level executive. While some companies have begun creating the position of "Chief Recovery Officer," usually the CEO or CFO manages the plan and assures buy-in from other executive-level staff.

Implementing a Business Continuity Plan

An effective business continuity plan is more than just the result of effective backups and data replication. An effective plan must not only be based on sound knowledge of your organization's culture and structure, but also on well-defined policies and procedures that make the plan a part of your daily operations, rather than something that is referred to only in case of emergency.

Your business continuity plan should include policies regarding:

- **Emergency response procedures,** such as reporting and tracking.
- **An executive communication plan,** with information on communicating with organizational management and other stakeholders, if applicable, as well as what your organizational response will be if key leaders are incapacitated or unavailable.
- **A public relations plan**, determining who will speak with the media.
- **Damage assessment and insurance claims processing information.**
- **An employee communication plan.** How will you communicate with your staff if mobile phone, landline and other communications networks are destroyed? How will you locate employees to share crucial information with them? Also, your organization should have a plan in place to manage critical personnel data, such as emergency contact information, user IDs and network passwords, in case systems are down or destroyed.
- **A communication plan for clients and vendors**, because you don't want to lose contact with either group, especially if operations are disabled for a period of time.
- **Banking,** especially regarding payroll and emergency cash access. This is an area that is particularly essential and challenging during a crisis, but is probably most overlooked when planning for a disaster. If you can't access funds during a crisis, your operations will grind to a halt, and disaster relief funding may not be immediately available.
- **Human resources systems that may not be immediately mission-critical,** but will become important in the weeks or months until operations are back to normal. Consider back-ups of salary information, payroll information and personnel and tax information as well.
- **A plan to handle phone calls, Website updates, e-mail and physical mail delivery.** What if your building is destroyed and there is no office to deliver mail to? How will you update your Website if your network is disabled?

When designing your organizational business continuity plan, you should consider the full dimensions of your organization's operations, including not just IT, but also business processes, staff and compliance. Of course, the plan must be updated and upgraded periodically to ensure it still reflects the realities of your organization. And finally, don't forget funding—**only 6% of IT budgets are allocated to business continuity.**

The steps and phases of business continuity planning follow logically from the determination of what risks are most likely to affect your organization, given your industry and physical location. If you are on the Gulf Coast, you are more likely to be hit by a hurricane than an earthquake. When considering risks, think outside the accepted natural disasters and don't forget to consider things like civil unrest, sudden changes in demand or hardware failure. For a complete guide to determining what disasters should be factored into your business continuity planning, please consult the first section of this white paper, "Defining Disaster."

Implementing Your Plan

Be sure to consider the following:

- Workload division
- Hardware alignment/positioning
- Storage strategy
- Data replication strategy
- Recovery and availability strategy
- Network connectivity and capacity measures
- Shared services and infrastructure components for base operating capabilities
- Virtualization alternatives
- Systems management mechanisms, command/control mechanisms, testing capabilities, physical and logical security features

A gap analysis of needs and capabilities will help you determine, in a high-level way, how able your organization is to meet the basic requirements of business continuity:

- Maintaining continuous business operations.
- Achieving regulatory compliance and meeting industry standards more quickly and cost-effectively.
- Integrating risk strategies to optimize resources.
- Providing data protection, privacy and security.
- Achieving and maintaining operational planning.
- Maintaining disaster readiness and preparedness.

Once you have identified your organization's particular needs and capabilities, you can design a strategy to mitigate the identified risks and integrate both business and IT objectives into the plan. The plans and procedures you design should then be tested—along with your system architecture—to assure that your business continuity strategies will have the desired effect.

As a reminder, **these plans are not static, and must be changed, evaluated, adjusted and tested on an ongoing basis.** You should test and reevaluate your business continuity plan frequently, employing rotating technical staff to ensure that recovery efforts are not halted if key personnel are absent.

Digital Document Management as a Part of Your Organization's Business Continuity Plan

Although most discussions of business continuity planning and disaster recovery planning focus on information that exists in electronic form, it is equally important to consider paper-based data. According to IDG Research, **80% of survey respondents indicate that they are considering or evaluating technology services to enhance or replace their current business continuity plan.** The leading approaches are storage replication, virtualization, redundant data centers, fail-over and electronic replication.

While most organizations are quick to consider their IT infrastructure when planning for a disaster, it is easy to forget paper archives. Paper is a familiar, yet extremely vulnerable, archival medium, particularly threatened by fire, flood and theft, and may be just as important as your electronic records, especially when it comes to pre-computer historical archives. While most, if not all, electronic records are backed up in some format, paper records are often forgotten—and once they are gone, they are gone forever. Some organizations duplicate records for off-site storage in an attempt to secure their paper records, but this is both time-consuming and expensive.

The solution is digital document management technology. With digital document management software, a digital image of your paper record is captured and preserved in unalterable format, guaranteeing its integrity. **Digital document management applications also manage your electronic documents—ranging from Microsoft® Word®, Excel® and PowerPoint® documents to Outlook® e-mails and digital audio and video files—from the same interface, providing a secure storage and recovery solution for both your paper and electronic documents.** Quality digital document management solutions enable you to convert both types of records to non-proprietary TIFF and ASCII formats and store them alongside imported electronic documents, providing for long-term access and security. Easily searchable and much more space- and cost-efficient than paper archives, digital archives can become a key factor in your organization's data storage and recovery planning.

Digital document management solutions can play a part in your organization's business continuity plan, by assuring that company records and documents are properly maintained and accessible when needed. This fits in with the emerging approach of "**recovery management,**" which leverages disk-based technologies to meet user needs. Digital document management solutions can tie into your organization's other IT solutions; for example, with CD/DVD publishing, your key documents will be available to your crisis team, even while your network remains down. Storing these disks offsite keeps data secure, enabling work to continue even if your offices are destroyed or your network is disabled. Quality digital document management solutions not only allow you to easily transfer your records to CD or DVD, but equip them with integrated viewers and search solutions, so you will be able to access your records from any computer—regardless of whether document management software is installed.

A back-up of your information, stored securely off-site, provides a relatively easy way to secure your data. **With digital document management technology, you assure data back-up and recovery while easily maintaining information off-site.** Without access to your data, key steps of your business continuity plan cannot be carried out and there is little hope of recovery.

Conclusion

An effective business continuity plan must not just protect employees and physical resources, but also protect the integrity of your organizational information, especially if it is confidential, sensitive and critical to business continuity. **Digital document management helps secure data integrity, comply with government regulations, integrate risk strategies to reduce costs and scale rapidly as your organization changes.**

Despite its familiarity, paper is a vulnerable archival medium. Easily damaged, easily lost and not easily replaced, it can present a sizeable obstacle to any business continuity plan concerned with the preservation of documents and records. Because these documents represent a crucial asset to most organizations, digital document management has an important part to play in business continuity plans. Digital document management technology enables your organization to create a centralized repository to store all vital organizational information. The method of storage can vary from off-site back-up to a redundant, mirrored site separated by geography, drawing from separate water and power grids. Effectively delivering on a continuity plan will not only enhance your ability to recover from a system failure, but will also help you to better define which records are crucial to your organization and improve your overall records management strategy.

Laserfiche®
Institute™

The Laserfiche Institute teaches staff, resellers, and current and prospective clients how to use Laserfiche most effectively. As part of this mission, the Institute conducts more than 500 Webinars each year, covering a variety of topics. The Institute also hosts an annual conference where members of the Laserfiche community attend presentations and network with each other to share ideas and learn best practices. Additionally, the Institute conducts a number of regional training sessions and provides resellers with content for over 100 user conferences each year.

The Institute also develops and distributes educational material through the Laserfiche Support Site. On this Website, clients can access training videos, participate in online forums and download technical papers and presentations that help them become even savvier Laserfiche users.

For more information, contact:
info@laserfiche.com

Laserfiche
3545 Long Beach Blvd.
Long Beach, CA 90807
United States

Phone: 562-988-1688
Toll-free: 800-985-8533 (within the U.S.)
Fax: 562-988-1886
Web: **www.laserfiche.com**