The Crucial Role of Vital Records in Business Continuity/Disaster Recovery

Published by:
Cennox

"The Crucial Role of Vital Records in Business Continuity/Disaster Recovery"

WHAT IS A BUSINESS CONTINUITY/DISASTER RECOVERY PLAN?

The chaos and confusion that follows a fire or other disaster is quite enough for a business to deal with. As evidenced by the events of September 11, as well as any number of accidental fires and explosions, simple survival may be the priority for an indefinite period of time. Once the immediate risk to human life is contained, however, focus must be centered on ensuring the continuance of business. However, when no formal master plan exists, decision-makers, (at the precise time when they need to be thinking as clearly as they possible) typically react in one of two ways: frantic scrambling or paralysis. Both of which translate into lost customers, lost revenue, and possibly, further damage to life and property.

A Business Continuity/Disaster Recovery (BC/DR) plan serves as the main resource for the preparation for, response to, and recovery from, a disaster that affects any number of crucial functions in an organization. A BC/DR plan provides a framework for the decisions made and actions to be taken by company officials in order to insure that operations can continue while the incident is occurring. In addition, the BC/DR plan serves to ensure that companies will be able to recover and return business activity (hopefully) to pre-incident levels.

It's not all about planning for the worst, however. Its good business sense - during the course of developing a good BC/DR plan your are likely come up with some good information and data needed for high level business strategy decisions, such as determining and prioritizing your critical business applications.

Senior management, as part of the holistic risk assessment and management process, uses various tools and methods for determining the likelihood of a disaster and its financial impact on an organization. Once organizations identify their risks in a value-related way, they will be a position to minimize the damage and put systems in place once an interruption to business continuity does occur. Having a BC/DR plan in place ensures that the organization can sustain losses stemming from the interruption or disaster.

WHO NEEDS ONE?

Every organization, large or small, public or private, whether you're located in a downtown business center or a suburban office park, (or even an office in the home) can and should look to improve their ability to survive and recover from a major business interruption. The good news is that it can be done without blowing up your operational budget. Nonetheless, developing a BC/DR strategy is not something that can be done "cheaply," nor should you think in those terms.

If you have the idea that an extensive BC/DR plan is an afterthought, not a priority, you are not alone, unfortunately. The National Federation of Independent Businesses, a small business advocacy group, conducted a survey recently, and found that 76 percent of all small business owners believe that insurance will adequately protect their business in case of

emergency or disaster. The Fortune 500 types, surprisingly, don't fare much better. According to the analyst firm META Group, fewer than 25 percent of Global 2000 enterprises currently have comprehensive, effective enterprise-wide business BC/DR plans that are adequately documented and regularly and rigorously tested to meet the rapidly changing demands of the business.

This we'll-get-by-without-one mentality is dissipating, stemming from an overall increase of the awareness of threats post-9/11 and the witnessing of several firms who, though initially devastated by the terrorist attacks, deployed their BC/DR plans to the fullest and went on to recover and even thrive beyond the most optimistic expectations.

According to Rick Sorely, President of Safetyfile Inc., "the greatest increased post 9/11 awareness regarding the need for firms to develop a disaster recovery strategy, seems to have centered on the small-to-medium businesses with 20-200 employees, generally, with one or more locations. Typically, a BC/DR plan may have been developed, but until now, it has never been fully funded or implemented."

Still, though, the real force driving business continuity is various business-governance apparatus (regulatory, insurance, legal) that compels executives to develop business continuity plans.

HOW TO GET STARTED DEVELOPING A BC/DR PLAN

The foundation for developing a contingency plan lies in developing a method for the protection and preservation of vital records. All businesses, especially small to medium sized organizations, should facilitate a proactive rather than a reactive approach to disaster preparation - especially with respect to vital records. Take the initiative and put a structured process behind vital record protection.

THE FIRST STEP IN DISASTER PLANNING IS VITAL RECORDS PROTECTION

Data is of course critical to a business, and installing a process for the storage of (and retrieval of) data is considered to be a basic operational requirement for all businesses. In the end, the fate of all businesses relies on data. Since the US economy is mainly a service economy, mainly comprised of companies that provide services, as opposed to manufactured goods, information and data are the key assets that need to be protected. That being said, traditional companies that manufacture and distribute physical products still need to have proof of loss to get any money back from their insurers - they absolutely need to have that proof to get paid on a claim after a disaster. For manufactures, there is also the element of protection of product design records - that if lost, would prevent them from producing their wares during the recovery.

This section will cover the most essential component of the BC/DR plan, the identification and protection of vital records. If a vital record is lost, damaged, destroyed or otherwise rendered unavailable, that loss becomes a disaster-within-a-disaster, affecting critical operations needed to recover from the initial disaster. Therefore, protection of vital records should be the

main priority (after the protection of human life of course) for contingency and recovery efforts when a disaster occurs.

Most fire protection, in the form of alarms and sprinklers, is designed primarily for life safety. Vital records protection is about mitigating loss and limiting property damage. Two very different concepts, which need to be viewed from different perspectives. Fire protection with regards to saving lives is not really a component of a BC/DR plan.

To state it as simply as possible, the first step in disaster planning is records protection. The safeguarding of vital and irreplaceable company records and documentation is absolutely crucial to corporate survival. If vital records that fall into certain categories, such as financial documentation records or sales orders - are lost, and can not be replaced quickly enough, a company could lose serious business as competitors move in to grab market share.

In fact, all businesses that have something to lose need a vital records protection strategy plan, and one that especially incorporates measures to protect against fire. To lend some perspective to the question of how much are your vital records worth, according to statistics from the National Fire Protection Association, 47 percent of all businesses that suffer a catastrophic fire cease operations inside of one year. Ninety percent of those firms whose records are destroyed are no longer in business a year later.

ASSESS THE THREAT TO YOUR VITAL RECORDS

So, in order to develop a vital records protection strategy, you must first assess the threats to your vital records. The first step is to identify specific risks, such as: facility and equipment hazards that can result in flooding to records storage areas, risky storage practices that increase the risk of fire, and periodic electric storms or tornados that could endanger digitally stored vital records. With electronic data you also need to consider poor care or storage - simple things such as spilled coffee, poor handling, etc.

During the past several years the United States has seen many natural and man-made disasters including major fires, hurricanes and floods. The loss of a company's vital record records due to fire can occur as a result of man-made or natural causes, however, regardless of the cause, the final outcome can be a devastating. According to that latest numbers released by the National Fire Protection Association, excluding the 9/11 incidents, fire damage caused $8,874,000,000 of property damage in structure fires in 2001.

The common element in each strategy, however is ensuring high levels of fire and security protection in storage containers and spaces, whether you choose on-site or off- site storage (more on that choice later.)

DEFINING WHAT DATA CONSTITUTES A VITAL RECORD TO YOUR ORGANIZATION

This is where organizations need to differentiate between important corporate data (which needs to be managed, stored and protected to some degree) and a vital record - defined as any recorded data that is essential for the survival of and continued operation of any

organization.

It would be foolish and costly to attempt to protect every bit of data to the utmost. To determine an effective-yet-cost-efficient strategy, set out to determine which data constitutes a vital record to your organization. First, audit and review your business processes and activities, then figure out what your most critical functions are, then identify those records needed for the performance of those functions. Next, take the process a step further and identify which records are required to support both those critical functions and the reconstitution of normal operations in the event of a business interruption. (Remember to assess all records, including electronic records.) To put it a bit more formally, identify which records series or electronic information systems contain information necessary to protect the legal and financial rights of the company and persons affected by the company's actions.

Vital records typically make up a small percentage of the vast amounts of recorded data, which is created by a typical organization, normally 5%. The range can vary, however, from 3% to 10%, depending on the business of the organization. However, a legal, medical, accounting and/or governmental organization may have a much higher proportion of active case files which are regarded as vital records.

Every business and every organization is unique, however the type of and level of value of your business's vital records will determine the amount of protection you should seek. Categories of recorded data that typically fall under the category of vital may include:

- Contracts/agreements that prove ownership of property, equipment, vehicles, products, etc.;
- Operational records such as current or unaudited accounting and tax records, current personnel and payroll records, client account histories and shipping delivery records;
- Current client files;
- Current standard operating procedures (SOPs);
- Produced reports and summaries;
- Software source codes, to include both licensed programs and systems and custom developed applications and registration keys.

DEFINING WHAT DATA CONTINUED

The above list should be considered a basic starting point. Next, consider: Although a specific category of records may not be deemed to be vital, it does not automatically mean that that type of record is not worth protecting. Ira Semanoff, a vice president of Top Hat, a corporate video production house in Bucks County, Pennsylvania, offers the following example. " Let's say a company spends $500,000 to produce a video, be it a commercial, a how-to or a training video. Usually, the master copy is kept at the production house, such as ours." Semanoff

continues: "If we were to suffer a fire, hundreds of master copies of various high-cost videos would be destroyed, representing millions of invested marketing budgets."

Each must be analyzed and tiered to determine the amount of protection you should provide. If not vital, you may determine non-vital (but valuable) records to be classified as:

1) Important records: not irreplaceable but could be reproduced only at considerable expense, time and labor;

2) Useful records: records that, if lost, will cause some inconvenience but could be readily replaced;

3) Non-essential records: those records which are in line for routine destruction.

In order to validate the classifications, those responsible for the vital records program should interview the managers and personnel who create records. Making for an excellent argument to justify outsourcing the development of the BC/DR plan, it is important to remember that most business managers will consider most, if not all, of their records to be in the vital category.

Fortunately you do not have to implement this crucial element of the BC/DR plan in a vacuum, for there are a number of standards bodies and organizations, most of which have a good amount of information publicly available on the Internet. These standards apply not only to the vital records themselves, but the actual facility and vaults housing the vital records and data recovery equipment as well.

(A full list of standards bodies and organizations follows at the end of this article.)

APPROACHES TO VITAL RECORDS PROTECTION

So, you've analyzed, reviewed and audited your company's storage needs and laid out in great detail what constitutes a vital record for your organization. You're not out of the woods yet, however you're still ahead of the game. According to a survey administered by the trade magazine Disaster Recovery Journal, only 25% of the vital records protection plans reviewed in the survey even addressed how the vital records were to be protected.

Some potential approaches for protection of vital records include: onsite fire-rated vault, safe or file cabinet, offsite storage at another location of the organization, and storage at a vendor that specializes in offsite vital records storage. Most companies employ various combinations of the above approaches. A major factor that will influence your decision is what medium the data is stored on.

KEY ISSUE: WHAT MEDIA TO RECORD AND STORE YOUR DATA ON?

Additional protective measures are needed for vital records maintained on a medium other than paper. These "special records" will require specific environmental conditions (including temperature and humidity controls) and careful handling throughout their life cycle, in order to ensure their preservation. Phillip Byrnes, as director of IT for Peabody, Massachusetts-based

manufacturer Synventive, is specifically responsible for protecting vital records that are stored on magnetic tape - and since he stores the majority of data onsite, he therefore had to seek a "data safe" that was specifically designed to store and protect data stored on magnetic tape.

Vital records can include many different media aside from paper, such as:

Microfilm
Microfiche
Optical disk
Magnetic tapes
Disks Cassettes
CD ROMs
DVDs
Photographic materials
Other media

For the majority of companies, magnetic tape is the storage medium of choice for archived data, since it has a long shelf life, usually a couple of decades.

Specifically designed data cabinets and vaults can be used to provide on-site protection for magnetic tapes and disks. For example, vital records can be protected against theft and fire by storing them in fire resistant safes or vaults with combination or electronic locks.

Remember, fire resistant file cabinets for paper and microforms do not provide sufficient protection for magnetic tapes, disks and diskettes, since the ignition point of paper and microfilm is much higher than magnetic media. They need to be stored in vaults that hold the temperature extremely constant during a catastrophic fire. Paper is destroyed at 400 degrees Fahrenheit whereas computer media is rendered useless at 125 degrees Fahrenheit. humidity (80% relative humidity)

The basic lack of awareness that leads to the destruction of many vital records and media involved in a catastrophic fire is that most don't understand the difference between a fire rating versus a classified fire rating. This simply means that the vault will protect the media stored inside it for at least two hours, and that the product has been tested and classified by Underwriters' Laboratory (UL) or another independent testing lab.

KEY ISSUE: ONSITE VS. OFFSITE

On the surface, it may seem to management that the simplest solution for the vital records program is to opt to store records offsite. This is a deceptively attractive option, because it looks like a simple solution to a complex problem. A plan that involves mostly onsite storage is, in fact, the preferable approach for all but the biggest and most regulated industries, such as financial services or health care.

The overwhelming trend is more and more companies are shifting to a combined onsite/ offsite approach -- what Van Carlisle, CEO of FireKing International, has described as a "belt

and suspenders approach." Even with this combined approach, the emphasis, however, is on onsite storage, for many reasons, including quicker retrieval, lower cost, and increased control. For example, many companies that used to have daily or semi-weekly pick-up by an off-site storage facility have moved to a monthly or semi- monthly pickup and expanded or improved their on-site storage, thereby simultaneously lowering a monthly expense and purchasing an asset {i.e. a data safe}

So, offsite storage of vital records can be a viable option for archived records, however, but for current information, such as daily backups and transaction records, storing vital records offsite requires such a high degree of discipline and coordination that it will become extraordinarily expensive and time consuming to try to move daily backups to an offsite location. At the end of the day, its just not feasible to rely 100% on offsite. The question remains: how do you ensure your vital records are secure while they remain onsite?

For daily backups, keep them onsite in a secure, fire-protected location, in a fire resistant file or vault, and for archival (such as annual, monthly or even weekly backup) records, supplement that backup with offsite. At the end of a predetermined time period, (say one month) run two copies - one off, and one on site.

So you still may need to pick a vendor that offers offsite storage. In the process of doing due diligence while researching offsite options, ensure that you get a complete understanding of all charges including: in and out, privacy and security, ask what type of care is used in transport, what type of facility is it -- is it truly in a vault? Is computer media stored separate?

At any rate there are some universal factors to consider:

- Distance - the facility should be located far enough away from the organization to ensure that a major disaster would not heavily impact both locations;
- Accessibility - the facility should have decent access roads, 24-hour access, and be accessible within a reasonable period of time so that the records can be obtained quickly;
- Safety - high-risk areas should be avoided, to include proximity to airports, railroads, chemical plants, flood plains, tornado belts, etc.
- Level of Service - some vendors provide courier service, photocopying, notary services, conference rooms, tape rotation, cleaning, maintenance and destruction;
- Security - rural and low-traffic areas can be more secure and easier to guard.

Lest anyone still think "out of site, out of mind," you still run a considerable risk with offsite storage, especially from fire. Below are a few recent vital records offsite storage fire-related disasters: *

10/26/96
Brambles Information Management Center in Chicago, Illinois
220,000 boxes of archival and vital records information destroyed by fire

3/7, 3/17 and 3/19/97 --Fire
Iron Mountain Record Centers in South Brunswick, NJ
Nearly 1 million boxes of paper records destroyed by fire, 200 companies affected

5/6/97 -- Fire
Diversified Records Services Center near Scranton, PA
Steel building the size of football field packed with paper documents and microfilm burns to the ground

*Source: Abbey Publications - a nonprofit corporation to encourage preservation of library & archival materials, and the use of lasting materials in the creation of records.

These facilities were all billed as "state of the art." Unfortunately, that usually means cardboard boxes in an open warehouse with a sprinkler system. The sprinkler system is the total protection of the records. You should inspect the vault facility and ask for specifications on the vault chamber, and the vendor should be able to provide the shop drawings and performance standards for their vault. Be wary of vendors with alliances or cross-selling deals with your microfilming services and storage vendor, who may not have your ultimate best interests in mind.

Company officers need to make the decision, based on cost and service factors, whether on-site records storage is the preferred method or if selecting an off-site storage facility is the way to go.

As mentioned, whether you go with on-site or off-site, the first action to take is to procure fire resistant safes and filing cabinets for on-site storage, as you will always, at one point, have vital records on-site, and obviously, no one is able to accurately predict the precise time a business interruption will occur.

If you opt to store vital records onsite, standard filing equipment is believed to offer fire protection by a large majority of consumers. This thinking, attractive to management because it "seems" cheaper, is erroneous and potentially dangerous. Remember, your attempting to protect your most vital information assets, and it is highly advisable to seek the highest quality. Price should not be an overriding factor in your decision. It is imperative to seek products that are tested by Underwriters' Laboratory (UL) or other nationally known independent testing labs - absolutely steer clear of equipment with manufacturers' or non-independent ratings. UL, in particular, is the best, as no other testing and standards organization matches their reputation. One "trick" to be wary of is a product that claims to be "built to" a certain UL class specification claim. This is marketing-driven wordplay, pure and simple - and it leads the

customer to falsely believe they are getting a UL rating, but in reality it's just the manufacturer's dubious claim -- UL has never tested it, and how it will stand up to a real fire is anyone's guess. Mark Fulton, a company official at Virtual Insurance, and underwriting firm in South Florida, says his decision to purchase a Cennox data safe was fully informed by the UL logo, in fact, Fulton claims that he "doesn't buy so much as a lightbulb" unless it is UL tested.

You won't have to sacrifice aesthetics for safety, either, as the top vendors in the industry offer well-designed attractive media rated safes, fire resistant file cabinets and fire safes for onsite records protection. You can readily find this equipment at your local office products dealer, in most office products catalogs, or increasingly, on the Internet.

KEY ISSUE: RECOVERY OF THE VITAL RECORDS IN THE EVENT OF A DISASTER

The final key element of the overall vital records approach is the recovery strategy. This should be based, of course, on a thorough and detailed knowledge to include the location of vital records (both onsite and offsite), and the level of information contained in master lists and indexes.

The "best practices" procedures for the removal of vital records in the event of a disaster should include prioritization of specific categories of vital records in the event of a recovery mission, a tracking plan, designation of one or more secure relocation destinations, primary and backup transportation arrangements, the offsite vendor's 24- hour contact information, necessary clearances and permits, and contact information for internal personal assigned to accompany the records - the responsible party must also be trained on the handling and preservation techniques based on the specific media involved.

CONCLUSION

On September 11, 2001, the immense amount of vital records that were incinerated and blowing around the streets immediately after the attack served as a wake up call. Companies that were totally unaffected (in a business, not personal, sense) by the terrorist attacks were shaken from their false sense of security about the need to evaluate and or implement a vital records program. It doesn't have to be a terrorist attack; it can be a simple case of a disgruntled destructive employee, a fire, flood or other natural disaster.

The key is to plan and develop a BC/DR strategy with a strong element of vital records protection BEFORE something happens, because once in the throes of a disaster, it's far too late.

STANDARDS ORGANIZATIONS

Below is a listing of some standards organizations and their standards and ratings:

UNDERWRITERS LABORATORY

333 Pfingsten Road
Northbrook, IL 60062-2096 USA
www.ul.com

Underwriters Laboratories Inc. (UL) is an independent, not-for-profit product safety testing and certification organization. UL has tested products for public safety for more than a century.

AMERICAN NATIONAL STANDARDS INSTITUTE

1819 L Street, NW
Suite 600
Washington, DC 20036
www.ansi.org

ANSI is a private, non-profit organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system.

FACTORY MUTUAL INSURANCE COMPANY

1301 Atwood Avenue Johnston,
Rhode Island 02919
www.fmglobal.com

Large, global network of commercial and industrial property insurance and risk management organizations specializing in engineering-driven property protection.

AMERICAN SOCIETY FOR TESTING AND MATERIALS

100 Barr Harbor Drive,
PO Box C700
West Conshohocken, Pennsylvania,
19428-2959
www.astm.org

Non-profit organization that provides a global forum for the development and publication of voluntary consensus standards for materials, products, systems, and services. Over 30,000 individuals from 100 nations are the members of ASTM International, who are producers, users, consumers, and representatives of government and academia. In over 130 varied industry areas, ASTM standards serve as the basis for manufacturing, procurement, and regulatory activities.

NFPA

1 Batterymarch Park
Quincy, MA 02269-9101
USA www.nfpa.org

The mission of the international nonprofit organization is to reduce the worldwide burden of fire and other hazards on the quality of life by providing and advocating scientifically-based consensus codes and standards, research, training and education.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
100 Bureau Drive, Stop 3460,
Gaithersburg, MD 20899-3460.
www.nist.gov

Non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurements, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.

####