



## All Records Are Not Created Equal

*Faced with a glut of data, businesses must rethink their vital records protection procedures.*

by Van Carlisle

文章简介：本文首先阐述了数据及其保护措施对于机构运行的重要性，接着描述了制定和实施关键数据保护策略的要点，包括对数据威胁的分析、关键记录的定义和保护措施的选择等方面的内容，最后本文还提供了一些相关资源的介绍。



[华安信达](#)

Data is of course a critical business need, and installing a process for the storage and retrieval of data is a basic operational requirement for every organization. For service companies, data is what makes the business go. And for manufacturers, while data isn't an end product or directly responsible for revenue, it is quite necessary for the continuity of operations. For example, manufacturers must have documentation to establish proof of loss if they want to see a return on an insurance claim following a disaster. Furthermore, consider the impact lost product designs could have on production during a recovery effort.

As such, identification and protection of vital records is a core element of the business continuity planning process. 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.

### **Fire Protection for Records**

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. These are two very different concepts, which need to be viewed from different perspectives. Fire protection as it pertains to saving lives is not really a component of a business continuity plan.

To state it as simply as possible, the first step in business continuity planning is records protection. The safeguarding of vital and irreplaceable company records and documentation is absolutely crucial to corporate survival. If vital records such as financial documents or sales orders are lost and cannot be replaced quickly, 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. 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 are out of business in two years.

### **A Burning Threat**

In order to develop a vital records protection strategy, the first step is to identify specific risks. For instance: 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 physical files poor care or storage must also be considered — 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. According to that latest numbers released by the National Fire Protection Association, excluding the September 11 terrorist attacks, fire damage caused \$8,874,000,000 of property damage in structure fires in 2001.

### **Defining a Vital Record**

Organizations need to differentiate between important corporate data (which needs to be managed, stored and protected to some degree) and a vital record. Defined, a vital record is any recorded data that is essential for the survival and continued operation of an organization.

It would be foolish and costly to attempt to protect every bit of data to the utmost. To develop a cost-effective strategy, a company must pinpoint its vital records. The first step in this process is to audit and review business processes and activities to determine critical functions. Once that effort is complete, an organization can identify the records needed to performance those critical function.

Next, take the process a step further and identify the records — electronic, physical or otherwise — required to support both those critical functions and the reconstitution of normal operations in the event of a business interruption.

In the end, vital records typically make up about five percent of the vast amounts of recorded data an average company has on file. The range can vary, however, from 3 percent to 10 percent, depending on line of business. Legal, medical, accounting and/or government organizations usually have a much higher proportion of vital records.

The type and value of your business's vital records will determine the amount of protection you should provide. Typical vital records include:

- Contracts that prove ownership of property, equipment, vehicles, and products
- Operational records, such as unaudited accounting and tax records, current personnel and payroll records, client account histories, and shipping delivery records
- Current client files
- Standard operating procedures
- Produced reports and summaries
- Software source codes for licensed programs and systems, custom developed applications, and registration keys

The above list should be considered a basic starting point. Although a specific category of records may not be deemed vital, it does not automatically mean that

that type of record is not worth protecting. Each record category must be analyzed and tiered to determine the amount of protection. If not vital, records can be designated nonvital (but valuable) and 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; or
3. **Non-essential** records — those records that are in line for routine destruction

In order to validate classifications, those responsible for the vital records program should interview the managers and personnel who create records. Keep in mind though, most business managers will argue that the majority of their records should be in the vital category.

Fortunately, there are a number of standards bodies and organizations that provide publicly available information on the Internet to assist in the process of developing a vital records protection plan. Some of the standards go beyond the vital records themselves and consider the actual facilities and vaults and data recovery equipment used for protection.

### **Protection Strategy**

According to a survey administered by the trade magazine *Disaster Recovery Journal*, only 25 percent of vital records protection plans address *how* vital records are 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 the decision is what medium the data is stored on.

### **Key Issue: Storage Medium**

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.

Vital records can be stored on a variety of different media, including:

- Microfilm
- Microfiche
- Optical disk
- Magnetic tapes

- Disks
- Cassettes
- CD ROMs
- DVDs
- Photos

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 onsite 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.

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" and a "classified fire rating." A classified fire rating simply means that something 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. 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 pickup by an offsite storage facility have moved to a monthly or semi-monthly pickup and expanded or improved their onsite storage, thereby simultaneously lowering a monthly expense and purchasing an asset (e.g. data safe, tape drive, etc.).

Offsite storage of vital records can be a viable option for archived records. However, 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, it's just not feasible to rely solely on offsite.

The question remains though, how can a company ensure the security of vital records?

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.

In the process of doing due diligence while researching offsite options, a company should make sure it has a complete understanding of all charges including: in and out; privacy and security; transport care, type of facility; and vaulting option. Also, an organization should find out if computer media is stored separately.

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, including 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 are more secure and easier to guard.

Facilities are often billed as "state of the art." Unfortunately, that usually means cardboard boxes in an open warehouse with a sprinkler system. When researching offsite facilities, always inspect the vault and ask for specifications on the chamber. The vendor should be able to provide the shop drawings and performance standards for the vault. Be wary of vendors referred by microfilming services and storage vendors. The referral may not be based on reputation, but rather a reseller agreement between the two providers.

Ultimately, company officers need to make the choose whether to store offsite or

onsite or through a combination of both based on cost and service factors. Regardless of the decision though, the first action to take is to procure fire-resistant safes and filing cabinets for storage, as vital records will always have a presence onsite.

Standard filing equipment typically does not offer fire protection. 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 nonindependent ratings. 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.

### ***Key Issue: Vital Records Recovery***

The final key element of the overall vital records approach is the recovery strategy. This should address the location of vital records — both onsite and offsite — and the level of information contained in master lists and indexes.

The 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 personnel assigned to given records, who must be trained on handling and preservation techniques based on the specific media involved.

### **Conclusion**

On September 11, 2001, a tremendous number of vital records were incinerated and blowing around the streets of New York following the terrorist attack on the World Trade Center. Unfortunately, on that day, companies around the world saw first hand just how important a vital records program can be. But a terrorist attack is not the only threat facing a businesses' vital records today. A simple case of a disgruntled and destructive employee, a fire, flood, or other natural disaster can also wreak havoc on vital records if they're not protected appropriately.

The key is to put an effective strategy in place before something happens that requires its use.

### **About the Author**

*Van Carlisle is president and CEO of FKI Security, a provider of loss prevention solutions such as fireproof files, safes, and digital recording equipment. Mr. Carlisle studied criminal justice at the University of Louisville and served six years in the Air National Guard Security Police Force.*

## **RESOURCES:**

### **Underwriters Laboratory**

333 Pfingsten Road  
Northbrook, IL 60062-2096

[www.ul.com](http://www.ul.com)

Underwriters Laboratories Inc. is an independent, nonprofit 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](http://www.ansi.org)

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

### **FM Global**

1301 Atwood Avenue  
Johnston, RI 02919

[www.fmglobal.com](http://www.fmglobal.com)

FM Global is a large commercial and industrial property insurer, specializing in engineering-driven property protection.

### **American Society for Testing and Materials**

100 Barr Harbor Drive  
PO Box C700  
West Conshohocken, PA 19428-2959

[www.astm.org](http://www.astm.org)

ASTM is a nonprofit organization that provides a global forum for the development and publication of voluntary consensus standards for materials, products, systems, and services.

### **NFPA**

1 Batterymarch Park  
Quincy, MA 02269-9101

[www.nfpa.org](http://www.nfpa.org)

NFPA is an international nonprofit organization that aims to reduce the worldwide burden of fire and other hazards on the quality of life by providing and advocating scientific consensus codes and standards, research, and training.

### **National Institute of Standards and Technology**

100 Bureau Drive, Stop 3460

Gaithersburg, MD 20899-3460

[www.nist.gov](http://www.nist.gov)

NIST is a nonregulatory 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.

**CORRECTION:** *Originally this article listed "FM Global" as "Factory Mutual Insurance Company." Factory Mutual Insurance Company is the legal name of the company. However, FM Global is the name it uses in the insurance marketplace. To avoid confusion, CPM changed the listing to read "FM Global" on April 16, 2003. Also, the company description for FM Global was clarified on the same date to show that it is a single entity, not a conglomerate of insurance organizations as was portrayed when this article was originally published.*