

Vital records protection: Guidelines for your firm

July 10, 2006

By Doug Voet

Would your company survive a devastating disaster or business interruption? This is a question that has been at the forefront of most business' concerns for a few years now, and one that needs to be continually asked in the future.

The foundation for developing a continuity and disaster recovery program lies in developing a method for the protection and preservation of vital records. All businesses, especially small and midsized organizations, should facilitate a proactive, rather than a reactive, approach to disaster preparation - especially with regard to vital records. This article focuses on developing a vital records protection strategy in the greater context of continuity and disaster recovery.

The Small Business Administration offers Business Physical Disaster Loans to businesses to repair or replace disaster damages to property owned by the small business, including real estate, machinery and equipment, and inventory and supplies. However, if your business is unable to produce the vital records that document the lost property because the records were destroyed in the disaster, any government assistance or insurance that the business may be eligible for can be seriously delayed or even denied.

Vital records are commonly defined as those records that contain information or data that is essential to the survival of an organization in the event of a major disaster or business interruption. They usually consist of a small percentage of the recorded data created by a typical small-to-midsized organization - normally around the 5 percent range, although that can vary depending on the business of the organization.

A legal, medical, accounting or governmental organization may have a much higher proportion of active case files that are regarded as vital records. However, in order to ensure compliance with a rapidly expanding amount of legal and regulatory requirements, such as Sarbanes-Oxley, Graham-Leach-Bliley and HIPAA, more and more electronic corporate data is being classified as vital.

In all cases, the accounting and financial functions will typically have a much higher percentage of active files and documents that are regarded legally as vital records, which in turn means that many senior managers are currently being prompted to evaluate cost-effective ways to upgrade their VRP procedures and record-retention policies.

Vital records need to be protected, as they document an organization's legal and financial positions and preserve the rights of employees, customers and stockholders in the event of a disaster. 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.

The first step of the VRP process is to define as specifically as possible what data constitutes a vital record for your particular organization. First, differentiate between important corporate data (which needs to be managed, stored and protected to some degree) and a vital record - defined previously as any recorded data that is essential for the survival and continued operation of any organization.

Audit and review business processes and activities, determine what the most mission-critical functions are, and identify the records that are needed for the performance of those functions. Next, identify which records are required to support both ongoing mission-critical functions and the recovery of normal operations in the event of a business interruption. (Remember to assess all records, including electronic records.)

In other words, identify which records series or electronic information systems contain information that is necessary to protect the legal and financial rights of the company and persons affected by the company's actions.

Corporate 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;
- * Produced reports and summaries; and,
- * Software source codes, including both licensed programs and systems, and custom-developed applications and registration keys.

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. Records that could be categorized as other-than-vital may include:

- * Important records: Not irreplaceable, but could be reproduced only with considerable expense, time and labor;
- * Useful records: Records that, if lost, will cause some inconvenience but could be readily replaced; and,
- * Non-essential records: Those records that are in line for routine destruction.

After the review and audit to determine what constitutes a vital record for your organization, the next step is to address how the vital records are to be protected.

The three main approaches for VRP include an onsite fireproof 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 small-to-midsized businesses will develop a program that uses various combinations of each approach. A major factor that will influence the decision is what medium the majority of the data is stored on.

In terms of the storage medium, note that additional protective measures are required for vital records maintained on a medium other than paper. These include temperature and humidity controls and careful handling throughout their lifecycle, in order to ensure their preservation.

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 and other media.

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

Whether protecting paper or other media, the one constant is to seek records storage products that are tested by the Underwriters' Laboratory or another well-known independent testing lab - avoid purchasing equipment with manufacturers' or non-independent ratings. UL-rated VRP equipment is readily available from most local office products dealers, in most office products catalogs or, increasingly, on the Internet.

The key element of VRP that ties everything together is the recovery strategy. This includes a prioritization of specific categories of vital records in the event of a recovery mission, insurance information, payroll and personal records, necessary clearances and permits, and contact information for internal personnel assigned to accompany the records.

So, you have analyzed, reviewed and audited your company's VRP needs and laid out in great detail a viable and cost-effective VRP strategic plan. The VRP plan is a work in progress, as new technologies emerge, along with new threats to the continuation of business. The key for the financial professional is to lead and plan and develop a VRP strategy before something happens, because once you're in the throes of a records-destroying disaster, it's far too late.