www.businessinsurance.com

Business Insurance®

As seen the week of:

March 31, 2003

Perspectives

Data-protection planning a critical task

By Van Carlisle

One crucial aspect of disaster planning is protecting vital company records. Information is, of course, critical to a business, and implementing a process for the storage and retrieval of data is a basic operational requirement for all businesses.

Because the U.S. economy is mainly a service economy, information and data are the key assets that must be protected. That being said, companies that manufacture and distribute physical products still need to have proof of loss to get any money back from their insurers, making data protection critical to them as well.

For manufacturers, there is also the need to protect product-design records that, if lost, would prevent them from producing their wares during a recovery period. 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 a central priority—after the protection of human life, of course—for contingency and recovery efforts when a disaster occurs.

Protecting vital records is about mitigating loss and limiting property damage. To state it as simply as possible, safeguarding vital and irreplaceable company records and documentation is crucial to corporate survival.

To state it as simply as possible, safeguarding vital and irreplaceable company records and documentation is crucial to corporate survival.

All businesses that have something to lose need a vital records protection strategy plan, particularly one that incorporates measures to protect against fire.

This is where organizations need to differentiate between important corporate data—data that must be managed, stored and protected to some degree—and vital records. A vital record is any piece of recorded information that is essential to the survival of the organization.

It would be foolish and costly to attempt to protect every bit of data to the utmost. To find a strategy that is both cost effective and sound, you should determine which data constitute vital records to your organization and develop a data-protection plan accordingly.

The first step is conducting an audit and review of your business processes and activities to determine what are your most critical functions. Once those functions have been identified, determine which records are essential to those functions.

Next, take the process a step further and identify which records are required to support both those critical functions and the resumption of normal operations in the event of a disruption. Remember to assess all records, including electronic records.

Every organization is unique, and the type of and level of value of your business' vital records will determine the amount of protection you should seek. Categories of recorded data typically considered vital include:

- Contracts and 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.
- Software source codes, including both licensed programs and systems and custom developed applications, as well as registration keys.

This list should be considered a basic starting point. Next, consider that although a specific category of records may not be deemed vital, that does not necessarily mean the data are not worth protecting. Each must be assessed to determine the amount of protection you should provide. Some types of records that may be considered valuable—but not vital—are:

- Important records—those that could be reproduced, but only at considerable expense, time and labor.
- Useful records—records that, if lost, would cause some inconvenience but could be readily replaced.
- Nonessential records—those 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 and keep records. It is important to remember that most business managers will consider most, if not all, of their records to be vital.

Fortunately, you do not have to implement this plan in a vacuum, as there are several data standards organizations that have a good amount of information publicly available on the Internet. These standards apply not only to the vital records themselves but also to the actual facilities and vaults housing the vital records and to data recovery equipment.

The vast amount of vital records destroyed in the Sept. 11, 2001, terrorist attack served as a wake-up call. Many companies that did not already have such a plan were made aware of the need to evaluate and implement vital-records programs. It doesn't have to be a terrorist attack that results in a loss; it could be a simple case of a disgruntled employee, a fire, a flood or any other natural disaster.

The key is to plan and develop a strategy for vital records protection before something happens. Once a disaster occurs, it's far too late.

Van Carlisle is president and chief executive officer of FKI Security Group, a New Albany, Ind.-based security and loss prevention firm.