Hanover Risk Solutions

Emergency Preparedness—Protecting Vital Records

Vital records, those necessary to ensure the survival of a business, should be protected from damage or loss. Indeed, for some businesses the information contained in business records is the most valuable asset. The loss of processing and trade secrets, drawings, formulas, and the like can cause significant harm to a successful business. This report provides information on developing a program to protect vital business records, as recommended by the Federal Emergency Management Agency.

Introduction

There are certain business records that are considered vital to any company—these can include the incorporation certificate, bylaws, stock record books, ownership and leasing documents, insurance policies, and financial records. While it is important to protect such records, there are other records that are important to the survival of a business in the event of a disaster or other event disrupting operations.

A manufacturing company, for example, would require engineering drawings and specifications, parts lists, work processes and procedures, lists of employee skills required, and similar information. Without these, it would be impossible to produce a product; and, for a complex product, the task of recreating all this information would be virtually impossible, especially in the short term. A financial institution, on the other hand, would require current information on the status of depositors' accounts, accounts with other banks, loan accounts, and related banking services.

This report outlines the steps involved in developing a program to protect vital business records, as recommended by the Federal Emergency Management Agency (FEMA) in the publication, *Emergency Management Guide for Business and Industry.*

Selecting Records to Be Protected

A records protection program is an administrative device for safeguarding vital information, not for preserving existing records. The following four-step procedure is suggested for analyzing a company's vital records:

Step 1—A project management team should be selected. The logical team leader is the company's records manager. Company operations should be classified into broad functional categories—while these categories will be different in each company, in general, they should include at least:

- **Finance:** bill payment, account collection, and cost accounting.
- **Production:** research, engineering, purchasing, and related activities.
- **Sales:** inventory control and shipping activities.
- **General administration:** personnel, legal, tax records, public relations, and similar staff activities.

continued ▸

Step 2—The project team should determine the role of each function in an emergency. Not every company function and activity will be essential to a timely, post-disaster recovery. Some activities may have to be suspended during the recovery period; others may have to be eliminated completely. If elimination or curtailment of an activity after a disaster will restrict the company's ability to restore some essential operations, then that activity is vital, and the information needed to maintain it is also vital and should be protected.

Step 3—The project team should identify the minimum information that must be readily accessible after an emergency to assure that vital functions continue to perform properly. For instance, to stabilize accounts receivables' collections, it may be necessary to have the most recent account statement of the outstanding balance at the time of the disaster, as well as a record of subsequent payments. Or, to clarify field parts inventory conditions, it may be necessary to have access to a copy of the most recent sales agents' reports.

This step may disclose that some of the records needed in an emergency are not created on a routine daily basis. In such a case, a system should be developed to assure that these records are available for post-disaster use.

Step 4—Finally, the team should identify the particular records that contain this vital information and the departments in which they are, or should be, maintained.

Protecting Vital Paper Records

Vital records may be protected by off-site storage of duplicate copies or be secured in protected onsite storage. While onsite storage in a fire-resistive vault or file room, fire-resistant safe, or record protection equipment, such as an insulated filing cabinet, may be acceptable for the storage of vital documents and records, these devices provide protection only for a limited period of time. A significant disaster could thus destroy the equipment, rendering the records useless, or damage or destroy the building, limiting access to these records. The off-site storage of vital records provides greater assurance that the information needed to reconstitute the business after a disaster would be available. Off-site storage in a record's facility located outside the risk area offers the advantages of quick retrieval from a single location, security, and air and humidity control.

In today's society, the majority of vital information is processed by computers and captured on computer media. In some businesses, however, certain vital information must be maintained as hard-copy paper records. The same planning considerations should be given to protecting both kinds of vital records.

For further information on equipment used to protect records, including computer media, sign in to Hanover Risk Solutions' Partners section and scroll down to E&S resources; click on Risk Management Information and search for Fire Protection Reports FP-33-01, *Fire-Resistive Vaults and File Room*, FP-33-02, *Record Protection Equipment*, and FP-33-03, *Fire-Resistant Safes*.

continued ►

Computer Information and Records

Effective protection of vital computer information is more complicated than safeguarding vital paper records for the following reasons:

- Company information is consolidated on the computer system, which intensifies its exposure to possible destruction.
- The data processing medium is extremely vulnerable to a wide variety of perils—fire, water, dirt, static electricity, transients (surges) over electricity and telephone lines, and hazardous chemical gases, to name a few.
- The electromagnetic pulse (EMP) from a nuclear explosion could produce damaging current and voltage surges in a data processing system, which could destroy the records. The most effective technique for minimizing damage to sensitive computer components from EMP involves isolating them electrically and/or magnetically from the EMP environment—by using transient protectors, for instance. In many cases, satisfactory isolation can be achieved by temporarily disconnecting equipment containing the sensitive components from power sources, antennas, or other input/output leads that enter the computer area.

  In cases where a company is totally dependent on the continued use of the computer to process information, there may be no option in the event of an emergency except to revert to manual processing of this data. Isolation by temporary disconnection may not be feasible. Thus, duplicate records, frequently updated, may be needed.
- Information transmitted for remote computer processing or handled by a computer service bureau is out of the company's direct control and custody for an extended period of time.
- The computer and the physical area in which it is located must be protected, along with the vital information that is so closely linked to it.
- The adequacy and validity of the programs used to process this information, and related computer operations' documentation, must be safeguarded to assure the usefulness, currency, and accuracy of the basic information.

Much of what already has been said about selecting and protecting vital records applies to records processed by a computer. Many of the general measures taken to protect vital data processing operations and records are measures that ordinarily should be taken to assure the general efficiency of the computer and its use by the company.

In protecting paper or microfilm records, it may only be necessary to safeguard the record itself. In contrast, in protecting vital data-processing records there are three distinctive elements: (a) the computer facility, (b) the physical data processing media, and (c) the inherent integrity of the information itself.

Protecting the Computer Facility

The following recommendations for improving computer facility security are not meant to cover every aspect of computer operations area design and layout.

- Make the central computer facility as inconspicuous as possible. Remove door and direction signs that identify the computer's location. It may be preferable to leave the computer facility entrances unmarked. Block off or otherwise eliminate display windows originally installed to permit exhibiting computer operations to visitors or those passing the building on the outside.

continued ►

- Strengthen controls over access to the computer facility. Provide 24-hour security guard surveillance of the area. In some companies, this may be supplemented by installation of closed circuit video surveillance equipment to permit monitoring of computer facility approaches. Install security hardware on all computer facility entrance doors. Maintain a record of all visitors—both outsiders and non-assigned company employees—and require that they wear a distinctive badge while they are in the computer facility. Encourage assigned employees to question visitors about their right to be in the facility, even when they are wearing visitor badges. Prohibit delivery by vendors directly to the computer facility.
- Review possible computer facility exposure to water and fire damage. Determine if the walls, ceiling, and air-conditioning system are sufficiently watertight to prevent possible damage in an emergency. Be sure that drainage under the facility's raised floor is adequate to avoid water accumulation wherever flooding may occur or water might be used to extinguish a fire. Install a dedicated heating and cooling system.

  Computer room fires are rare, but smoke damage from fire in adjoining premises is common. Reduce exposure to arson attempts by relocating HVAC air intake ducts from ground-level locations to the highest practical level above the ground, such as under the building eaves. Install an automatic suppression system, such as automatic sprinkler system, water mist system, clean agent system, or carbon dioxide system. Do not allow combustible materials, such as paper or cardboard, to accumulate in or near the computer facility. Prohibit smoking within the computer facility.
- If the computer facility is located in an urban, high-rise, controlled-environment building, consider the possible fire effects of two basic building construction features:
  1. Heat circulation openings between the exterior and interior building walls may encourage fire to spread by breaching fire walls, and
  2. Sealed windows may intensify heat buildup by offering no openings through which it might dissipate naturally.
- Provide an automatic emergency backup power supply. Attach an audible warning device to the emergency power source to assure that the computer operator and others are notified promptly of the shift to reserve power.
- If data processing is a critical business operation, have an alternate computer facility that can be used in an emergency. The alternate facility should have sufficient reserve processing capacity and mainframe schedule time to permit it to handle the company's work. Alternate computer facilities may be a duplicative company facility, either in-house or in an alternate headquarters, or various levels of facility backup from commercial firms.
- When processing, all computers emit very low-level electrical signals that can be detected by special equipment. A company may want to consider a Faraday Cage to shield vital information containing company secrets from external monitoring while it is being processed.
- Make sure that all unused wiring, including telephone cables, is removed from the computer facility. Make sure that heating and air-conditioning ducts and water pipes are grounded as close to the computer facility as possible. Both practices will reduce the likelihood of a tap being placed on the data processing system.

continued ►

Safeguarding Data Processing Media

Data processing tapes and disks containing vital information should be protected in insulated records containers that meet the testing requirement of UL 72, *Standard for Tests for the Fire Resistance of Record Protection Equipment*, published by Underwriters Laboratories Inc. Equipment that meets the requirement of UL 72 are Listed in UL's *Online Certifications Directory* (http://database.ul.com/cgi-bin/XYV/template/LISEXT/1FRAME/ccnsrch.html) under the category, "Record Protection Equipment (RYPH)."

Record protection devices are intended to provide protection to one or more types of records, according to specific classification ratings, as follows:

- Class 350 for paper. The temperature of 350°F (177°C) is regarded as a suitable limit for the safe storage of paper records.
- Class 150 for magnetic computer tapes and photographic film. The temperature of 150°F (66°C) is regarded as a suitable limit for the safe storage of computer tapes, photographic records, and other film-based media.
- Class 125 for flexible disks. The temperature of 125°F (52°C) is regarded as a suitable limit for the safe storage of flexible computer disks.

Each of these temperature ratings are further assigned an hourly rating, ranging from 4 hours to ½ hour, depending upon how long the device will prevent the inside temperature of the device from exceeding the rated temperature.

Vital computer records can be provided with additional protection by copying them onto duplicate media for storage at a remote location. To avoid possible fraud, these duplicate copies should be placed in the custody of the internal auditor at the location where they are stored.

Assuring Information Integrity

The integrity of computer-processed records is maintained by limiting data access to authorized users and then by careful control over data input and user file access, program content revisions, and computer facility operating practices. In each of these areas, some protection will be provided by normal data processing management practice.

Input and File Access

Input data editing routines can be designed to detect and automatically reject spurious information. Vital records processing programs also can be designed to selectively limit user access to key file segments and to restrict user ability to modify certain types of information in the file. In addition, the resident supervisor or operating system program should maintain a log inaccessible to assigned computer operators. This log should routinely record programs processed, files used, computer operator assigned, and use rate and elapsed time. Where the computer facility services a data transmission network, this log also should record user terminal identification, and the type of inquiry made. Computer facility supervisors and company security officers should review the log jointly at least once weekly and investigate questionable inquiries and apparent irregularities.

continued ▶

Program Content Revisions

Computer programs used to process vital information should be fully documented. A current copy of this documentation should be stored offsite. Programs purchased or leased should receive protection equal to that given to company-developed programs. Programs from outside sources may also have been adapted in some way to meet the company's specific data processing needs.

As company operating policies and procedures evolve, the programs used to process computer records must be altered to reflect these changes. Program changes should be fully documented; programmers involved in these changes must be clearly identified in the program documentation; and both the user department and computer facility supervision must review and approve these changes before they are implemented. Programmers must not be permitted on their own initiative to make even minor changes in the production programs they are running.

Computer Facility Operating Procedures

Computer operators should be assigned to work in pairs at all times, even on weekends and holidays, and especially when vital records are being processed. A supervisor or senior operator should be assigned to work with a less experienced person. Teamwork will improve overall operations quality and make it more difficult for operator errors or data alteration to go undetected. The possibility of file destruction through operator error can be reduced further in two ways: placing the operating or executive supervisory program in read-only memory—this will safeguard the program's memory protection feature, which will prevent accidental file segment destruction and block illegal file use; and instructing computer operators not to terminate or dismount any program until a satisfactory end-of-job message from the program has been logged in the console terminal.

Computer operator team assignments and work shifts should be rotated periodically to maintain separation of duties. As part of these same controls, an operator should not process the same programmer's programs for an extended period of time. Encourage operators to remain alert to facility physical condition changes. They should check periodically during each shift for such things as magnets, screwdrivers, files, and other small potential sabotage tools; disengaged security and fire alarm equipment; and open doors to operational disk units and other peripheral equipment.

Careful scheduling of computer time ensures more efficient use of the facility's capacity and makes it easier to spot diversion of computer time for unauthorized copying of vital information files. The schedule for processing particular vital records should be varied; the program should not be run at the same time every day or on the same day each week.

Certain information can be identified as vital only as long as it remains uncompromised by industrial espionage efforts. Extra steps should be taken to prevent compromise of the company's computer processed information. Carbon paper, impact printer ribbons, discarded forms and printout copies, and used tabulating cards should be destroyed in a document shredder located in the computer facility.

Special operating procedures for remote data transmission terminals will reduce the possibility of compromising vital information.

continued ►

Data sent over common carrier lines is exposed to interception through line taps. It can be reproduced in a tap-attached printer compatible with the data transmission system used. Addition of store and forward capabilities to the tap terminal makes it possible to hold the intercepted information and to modify it before releasing the information back into the system. Encryption programs used with data transmission systems make it possible to disguise vital records message content during transmission. Decoding at either end of the transmission link makes the input processible, or the program response understandable, at the remote terminal.

Personal Computers

Personal computers (PCs) and small business computers are more susceptible to data security breaches than large centralized or distributed systems. They are often located in an open area and are operated by non-technical users who use low-priced applications software. While these systems are often the first place data is entered in a large corporation before transmission to mainframe data storage, they are the only computers a small business may have. The information generated in this type of equipment is as valuable as that generated on any other type of equipment.

The problems in protecting data on PCs are complex. These problems include a lack of software reliability, data integrity, backup/recovery procedures, and physical protection (data disks can be duplicated easily). Also lacking is protection for data that is resident on a hard disk or in system memory. Further, there is no differentiation between public and private data sectors in small multiuser systems in which all files are currently available to all users. Care must be taken to backup and store data disks in remote locations from the site of the personal computer.

A number of tools, both software and hardware, to combat these problems are available. These include physical locks to prevent unauthorized individuals from turning the equipment on, as well as software locks, which require passwords to allow access to various applications.

Testing Protection Programs for Vital Records

The security officer, records manager, and internal auditor should test/evaluate the vital records program at least once a year and note any program defects or problems in a joint test results report to be sent to the proper company officer for information purposes and remedial action.

Determining Test Objectives

The test determines if the currently operated program will provide needed information under circumstances simulating disaster or emergency conditions. Every effort should be made to make test conditions as realistic as feasible.

Broadly, the tests should verify that vital records needed after a disaster are: (a) current; (b) protected sufficiently against natural disasters, nuclear detonation, and other possible perils; and (c) retrievable as needed in usable form. More specifically, the tests should determine that the company's various vital information needs can be satisfied in a typical emergency situation. As examples:

- Employees can be paid and proper deductions made for taxes, the retirement fund, and other payroll accounts.

continued ►

- The company's cash position and the location of its banked funds can be determined.
- The company assets, accounts receivables, and payable ledgers are all current.
- The order entry, engineering, production, and customer account information needed to resume production and sales activities are available and current.

Preparing and Conducting the Test

After scheduling the test, it should be determined where it will be held, who will participate, and how long it will last. Advance knowledge of the test date should be restricted to as few people as possible, and the test period should be kept as short as possible. The amount of time required for the test will vary—a large company may need several days to complete it, while a small company may need no more than an afternoon. Participants' absence from their regular duties should be kept to a minimum. The test should be located off company premises, if possible, to eliminate intrusion of normal day-to-day business matters. It may be held at a motel, an executive conference center, the company alternate headquarters site, or in a conference room made available by the local emergency management agency.

Well in advance of the scheduled test date, arrangements should be made for necessary test participant team support, working space, couriers, microfilm, copying equipment, and access to data processing equipment. Also, arrangements should be made for company executives who are familiar with the records used in the test, and not scheduled to participate in the test, to act as judges. They must be able to determine if the problems posed by the test have been answered successfully.

After the participants arrive at the test site, the test conditions should be explained, emphasizing that the problems posed must be answered by records currently included in the Vital Records Protection Program. The questions to the test team should then be given.

Typical Vital Records Test Problems

Assume that the facility has been completely destroyed during the night, with nothing salvageable. Demonstrate the company's ability to perform tasks, such as the following:

- Notify all managers to report to an emergency center for reorganization planning.
- Notify all other employees not to report to work until further notice.
- Continue paying company personnel on time.
- Send alternate shipping instructions to vendors with whom orders have been placed.
- Prepare a list of sources of supply for a specified product.
- Produce engineering drawings and the bill of materials for a small number of specific products.
- Prepare an insurance claim statement covering the complete destruction of the manufacturing buildings.
- Prepare a list of vendors in order to replenish operating departments.
- Produce a current statement of assets and liabilities and a statement of income and expense.
- Produce a list of commission balances for each manager and sales representative by employee number.

continued ▸

Allow time for the test team members to determine what records will be needed to answer the questions. As the requested records arrive by courier from their various locations, they must be reproduced or reconstructed in useful form. If the records are on microfilm, prints must be made of the first 10 images on each reel. These prints must be inspected by the test judges to determine that they are sufficiently legible for use in performing the specified test task. If the records are on computer magnetic tape, the test must print out successfully the first 100 records on each reel. The judges must determine that the printout adequately reproduces these records. Records used in the test must be returned by the couriers to their protected locations as soon as the test is over.

Testing Vital Computer Records and Operations

Vital computer records will be used to satisfy many of the basic test problems. But a comprehensive evaluation of the Vital Records Protection Program requires supplemental testing of vital records computer processing. Devise tests that will:

- Compare a clear copy of the tapes for selected vital records processing programs against a copy of the programs currently in use to determine that protected computer program documentation is current.
- Demonstrate that computer audit trails are being maintained in vital records computer programs.
- Determine that the alternate computer and its associated supervisory programs are still compatible with the company computer facility.

Other aspects of computer facility operations should be tested. These will be determined by company data processing management policies.

References

1. Emergency Management. *National Oil and Hazardous Substances Pollution Contingency Plan Overview*. Washington, DC: Environmental Protection Agency, September 15, 2008. https://www.epa.gov/emergency-response/national-oil-and-hazardous-substances-pollution-contingency-plan-ncp-overview.
2. Federal Emergency Management Agency. *Emergency Management Guide for Business and Industry*. FEMA 141. Washington, DC: FEMA, 2004. https://www.fema.gov/media-library-data/20130726-1511-20490-6446/bizindst.pdf

To learn more about Hanover Risk Solutions, visit hanoverrisksolutions.com

The Hanover Insurance Group®

The Hanover Insurance Company
440 Lincoln Street, Worcester, MA 01653

hanover.com

The recommendation(s), advice and contents of this material are provided for informational purposes only and do not purport to address every possible legal obligation, hazard, code violation, loss potential or exception to good practice. The Hanover Insurance Company and its affiliates and subsidiaries ("The Hanover") specifically disclaim any warranty or representation that acceptance of any recommendations or advice contained herein will make any premises, property or operation safe or in compliance with any law or regulation. Under no circumstances should this material or your acceptance of any recommendations or advice contained herein be construed as establishing the existence or availability of any insurance coverage with The Hanover. By providing this information to you, The Hanover does not assume (and specifically disclaims) any duty, undertaking or responsibility to you. The decision to accept or implement any recommendation(s) or advice contained in this material must be made by you.