

NFPA guides business professionals, governments, and property owners in the protection of essential records that are vital to the performance and survival of their vested interests.

permanent record

PROTECTING RECORDS: Post 9-11

Now more than ever, companies are recognizing that protecting records is a crucial part of business. ■ SCOTT BALTIC

THE MORNING OF SEPTEMBER 11, Bill Saffady was standing in front of his Brooklyn brownstone watching an inexplicable sight: slowly fluttering down from the beautiful blue sky were countless pieces of paper. There were tax forms and interoffice memos and unending scraps of who knows what.

"What's happening?" wondered Saffady, a university professor. One of his neighbors speculated that the papers had fallen from an aircraft, but that didn't seem plausible.

The answer, of course, was plainly and painfully visible across the East River from the end of Saffady's block: the attack on the twin towers of the World Trade Center in Manhattan.

"That whole day," Saffady marvels, "it was raining documents all over Brooklyn."

The human toll from the World Trade Center and the Pentagon attacks was their most terrible cost, but the business documents that gradually blanketed some New York neighborhoods represented the lifeblood of the stricken companies in the towers.

Business continuity, an organization's ability to quickly resume normal operations following a fire or other calamity, rests on many factors, not the least of which is ready access to important business records or usable duplicates. For the past decade, records protection has been increasingly recognized for its crucial role in business continuity planning. And since the September 11 attacks, many companies have taken a harder look at their vulnerabilities to the catastrophic loss of business records, both paper and digital.

"Business interruption equates to economic loss," says Mark Conroy, senior fire protection engineer and staff liaison for NFPA 75, *Protection of Electronic Computer/Data Processing Equipment*. "And the protection of records is vital to many, many companies."

First steps to a fix

"Your starting point is to see what needs to be protected," says Joe Flach, vice president

of Eagle Rock Alliance, West Orange, New Jersey, which consults with businesses on disaster recovery.

More specifically, Judy Bell, president and CEO of Disaster Survival Planning Network, Port Hueneme, California, asks clients to identify vital records, department by department, based on financial, legal, and operational needs. Once Bell's clients have identified which records are vital, the next questions she asks are whether these records have been duplicated and if so, whether the duplicates are safely off-site.

What makes vital records vital?

"These are the records that, if you didn't have them, your business couldn't operate," says Stephen E. Hannestad, director of the Space and Security Management Division, National Archives and Records Administration in Washington, D.C. He is also chair of the committee for NFPA 232, *Protection of Records*.

From the perspective of fire protection standards, determining which company records are vital is an unusual, perhaps unique, aspect of the process.

"Only the owner of the record can make the determination on how vital the record is," not the fire marshal or the fire chief, says David R. Hague, NFPA senior fire protection engineer and staff liaison for the NFPA 232 technical committee.

The flexible, even subjective, nature of these decisions is reflected in NFPA 232. For example, NFPA 232 allows a record owner—probably with input from the company's insurer—to define records as "vital," "important," or merely "useful."

The good news is that records-management consultants estimate that typically only 1 to 5 percent of a company's records are considered vital. Nonetheless, securely protecting them requires a commitment in a company of any size. That's why Flach emphasizes that a company needs an ongoing "vital records program," not a one-time vital records project.

Even identifying and finding all the data that must be backed up, duplicated, or otherwise protected isn't necessarily easy. Flach estimates that up to 10 percent of many companies' data is on individual employees' hard drives, not local-area networks.

Records protection is harder for some organizations to manage than others, says Doug Henderson, president of Disaster Management Inc., in Plantation, Florida, and one big factor is how much information is on the central data system. If many employees work at home on their laptops or if the creative department uses Macs instead of PCs, for example, records- or disaster-recovery managers will have to make sure they're included in the program.

In addition, "there are still a lot of vital paper records in the work environment that aren't accounted for," says Bell. "Vital records can be all over the board." One example she cites is minutes to board meetings, about which companies tend to forget.

Bell describes one company in the auto finance field that belatedly realized that the original "pink slips" (certificates of title) to the cars on which it held loans were simply stored in filing cabinets in scattered branch offices. After researching the costs and delays involved in replacing the slips, she says, the company decided to install a fireproof records vault in each branch.

Businesses should also know the various rationales for records protection, says Flach. A company's mission-critical data, the stuff needed to operate day to day, are usually backed up, he says, but archival data, such as tax records and other financial information, are also important, even though they may not be treated that way.

Companies must distinguish between ongoing backups for temporary data versus archival copies of information for long-term retention and protection, says Rainer Naus, corporate records manager for pharmaceutical maker AstraZeneca.

"A lot of people think a backup tape is a retention copy, but that's not true," he says. "They serve different purposes."

Finally, how long should important records be kept safe? That, too, depends, says Hannestad. Records showing the cost basis of property, for example, should be kept for as long as mandated by tax laws, while personnel

SINCE SEPTEMBER 11, MANY COMPANIES ARE TAKING A HARDER LOOK AT THEIR BUSINESS VULNERABILITIES TO THE CATASTROPHIC LOSS OF BUSINESS RECORDS, BOTH PAPER AND DIGITAL.



records might be retained for 20 years. If a company drops its bad debts after five years, that's another guideline.

Paper or plastic?

Though the digital revolution has permanently changed the business of managing and protecting business records, many companies remain heavily, sometimes unavoidably, dependent on paper.

"Many companies have a lot of dependence on hard-copy documentation," says Flach, and that isn't as well protected as digital data.

"The less reliance you have on hard-copy documentation, the better," he adds, but "it becomes an issue of cost" to digitize and back up paper records.

The bright side, says Bell, is that the cost of digitizing paper records "has come down tremendously in the past five years," encourag-

ing more companies to go that route.

Even before September 11, at AstraZeneca, there's more interest in electronically archiving records, says Naus, but there are also concerns over long-term storage of digital media. Even if a CD you burn today lasts as long as advertised, he notes, "what are you going to use to read it 50 years from now?"

The interest was high before the attacks on the World Trade Center and the Pentagon at aerospace giant Lockheed-Martin Corporation where they're moving toward more "dual protection"—tapes duplicated and moved off-site—says Janet Pomeroy, manager of records management, as well as more imaging of hard-copy documents into digital formats.

"We're definitely trying to move" toward an emphasis on digital records instead of hard copies, she says.

"Data migration is a huge area we need to look at."

Formed about six years ago by the merger of Lockheed and Martin-Marietta, Lockheed-Martin is in a situation to which many in today's fluid business world can relate. The corporate headquarters functions almost as a holding company for 40 subsidiary companies in four major business lines. It's no wonder Pomeroy is trying to consolidate or at least standardize numerous and varied legacy records systems.

Common problems

Not only must important business records be kept safe, but there must also be a plan and an infrastructure that allows the company to access and use them quickly. The ability to recover and access data from a separate site is crucial, yet under-recognized, says Flach. Based on his experience, he'd give business in general a grade of C+ to B on data backup; he thinks recovery plans currently merit no more than a C-.

This is one of the lessons learned from the World Trade Center and Pentagon attacks, says Brian Zawada, a business continuity planning consultant with GE Global Asset Protection Services. Some of the companies in the World Trade Center rarely tested their backup from tape, he says, and several later found the data unreadable.

Another reason to try out data-recovery plans periodically, says Alastair Brown, managing director of Rushbrook Consultants in

Glasgow, Scotland, is the frequent, ongoing change in business software.

Though having more protection than one needs isn't a grievous mistake, Flach says, some companies buy a product or service to protect vital records without a clear notion of what they're trying to protect or why. For example, the real-time data backup practiced by the financial-services industry is at the high end of the records-protection spectrum and not applicable for most companies. Instead of overbuying, he cautions, let your need drive the product or service, not the other way around.

Perhaps the most common problem with records protection described by those in the field is the failure to give it enough importance and fund it adequately.

"Businesses tend to want to ignore the issue," says Bell, because vital-records programs, though potentially company-saving, are also time-consuming and costly.

Since September 11, other disaster management companies are reporting more interest from potential clients.

Companies are running lean these days, says Ken Linder, assistant vice president of Loss Prevention Technical Services at GE Global Asset Protection Services, so contingency planning tends to be neglected.

"We talk about businesses operating on 'tribal knowledge,'" he adds, meaning the information that's locked inside people's heads and not recorded anywhere. Losing both essential people and large amounts of records in a single disaster, he points out, can hugely magnify the damage done to a company.

Some better than others

For various reasons, some types of businesses do well taking care of their records, while others typically don't.

"In our experience," says Bell, "financial institutions are the best, and law firms are the worst, the most vulnerable."

Flach agrees that financial-services companies do a good job, generally because of the government regulations they're subject to, and Henderson adds hospitals to the list of organizations that have to keep a lot of records and usually do a good job.

Another industry often singled out as better-than-average at records protection is the biopharmaceutical industry.

"Record-keeping is a key part of what we do in the pharmaceutical industry," agrees AstraZeneca's Naus. He notes that the company has had a good records program since it was formed in 1999 by the merger of pharmaceutical company Astra and specialty chemical maker Zeneca.

At AstraZeneca, essential research materials are routinely scanned and digitized, and the originals are then stored off-site. Similarly, researchers must periodically turn in their lab notebooks, which are microfilmed, then stored off-site under firm inventory control, so they can always be found.

The distance to the off-site storage isn't a key factor, Naus says, because AstraZeneca is headquartered in Wilmington, Delaware, an area that isn't subject to flooding, earthquakes, or hurricanes. But if the company were based in Florida or California, he thinks it would be wiser to store vital records farther away.

As a major defense contractor, Lockheed-Martin also has high standards for records management and protection, Pomeroy says.

Whatever the industry, says Henderson, technology departments fortunately tend to be more attuned to disaster planning. Often, he says, an IT department will have its own plan, even if the company as a whole doesn't.

Unfortunately, evidence suggests that other parts of the private sector can be far behind the curve.

Saffady, the Brooklynite who watched the paper fallout from the World Trade Center attack, teaches at Long Island University's Palmer School of Library and Information Science. He recently completed a survey of records-management practices among Fortune 300 industrial companies. Funded by the American Records Management Association (ARMA), the study is based on extensive interviews with 42 records managers who are also ARMA members.

Saffady found that, at least among industrial companies, records managers have a discouragingly low level of interest in records protection.

"It wasn't a priority for anybody," he says. "Nobody had anything to say about the protection issue."

Further, he found that only about 60 percent of the records managers he interviewed

are actually responsible for records protection. So who is? Saffady isn't sure, but suspects that it's a mix of security, IT—and maybe no one at all.

A safer future, or not?

Will vital-records programs begin to wither in a few years? Observers disagree on the future.

Henderson expects September 11 to have a lasting impact on records protection. Although funding for business continuity programs tends to be cut in down business cycles, he says, this area has been getting bigger in the last 10 years. And he's seen "a tremendous increase" in interest since September 11.

The business community's preparations for Y2K played "a pretty significant role" in getting records protection on people's radar screens, says Flach, but even something as momentous as the first World Trade Center attack "grows ancient." After September 11, a lot of companies reached back to their Y2K plans, only to find them out of date, Flach says.

He adds that, despite the fact that records protection is now a "boardroom issue" in more companies than ever, this function still competes for budget dollars with revenue-generating initiatives.

Zawada notes that the cutting edge of business-continuity programs is now where companies want their suppliers and other business partners to be, so that they, too, will be prepared for a major fire or other disaster. He also points out that many companies already have plenty of in-house knowledge that can help in records-protection planning if and when top management commits to a vital-records program.

Though all of his survey interviews were done before September 11, Saffady is skeptical that attitudes have changed significantly since then.

The World Trade Center bombing in 1993, the California earthquakes of the past decade, and Hurricane Andrew didn't wake the business community up to these issues; he doubts September 11 will have a major or lasting effect.

Though opinions differ on whether companies will actually establish and, equally important, support records-protection programs, the experts agree that the need is there—and never more so than now.

Says Henderson, "It's a form of insurance." ♦

TRIAL BY FIRE: Protecting Federal Records

The fire protection of federal records is rooted in scientific testing and real-life experiences. ■ **STEPHEN E. HANNESTAD**

SHORTLY AFTER MIDNIGHT ON July 12, 1973, a fire was discovered in a 200,000-square-foot (18,580-square-meter) storage area on the sixth floor of the National Personnel Records Center (NPRC) in St. Louis, Missouri. The reinforced-concrete building, which housed millions of files containing the personnel records of active and nonactive members of all branches of the U.S. military, had no automatic sprinkler system, and there were no partitions in place to halt the fire's spread.

Despite the efforts of 362 firefighters from 42 fire departments, the blaze burned out of control for more than a day, destroying the entire sixth floor and 18.5 million files. Another 21.7 million files were severely damaged. The fire destroyed 80 percent of the records for Army personnel discharged between November 1, 1912, and January 1, 1960. It also destroyed 75 percent of the records for Air Force personnel with surnames from "Hubbard" through "Z" who were discharged between September 25, 1947, and January 1, 1964. No duplicate copies of the destroyed records were maintained, nor was a microfilm copy ever produced.

In the aftermath of this fire, it fell to the U.S. National Archives and Records Administration (NARA) to reconstruct the information contained in the records. Twenty-nine years later, NARA continues to spend millions on the project annually.

Why we store federal records

Section 3101 of Title 44 of the *United States Code* requires the head of each federal agency to make and preserve records documenting the organization and its functions, policies, decisions, procedures, and transactions, and to furnish information necessary to protect the legal and financial rights of the government and those directly affected by the agency's activities. The length of time these documents

are retained is established by a statute of limitation or some other legal requirement, ensuring that the public isn't paying to store records that no longer have any value.

Most federal records are disposed of once they've served their statutory, fiscal, or administrative use. Typically, records are destroyed when they're superseded, become obsolete, or are no longer referenced. In many cases, this means that their retention period is relatively short.

However, some records must be kept longer. Such documents include federal contracts, which are retained for six years and three months after the final payment has been made. Other records, particularly those that provide evidence of a citizen's entitlement to a benefit, are kept for 50 years or longer.

Federal records that must be kept longer than three years are extracted annually from active office files and retired to a records center, where they remain until they're recalled for active use, reach their disposal date and are destroyed, or are transferred to the NARA for permanent retention. Approximately 3 percent of all federal records are designated "permanent" and will eventually be transferred to the National Archives in Washington, D.C.

Because federal records are so integral to the proper functioning of the U.S. government, NARA officials were determined never to suffer the devastating effects of another fire like the NPRC fire. To that end, the U.S. General Services Administration (GSA), the building's owner, established a blue-ribbon committee in 1973 to review every aspect of records protection in archives and records centers, from the structural design of the storage facility to the number of protective personnel on the site and the design of the fire protection systems.

Dr. Wilfred I. Smith, Dominion archivist of Canada, chaired the committee, and Charles S. Morgan, then

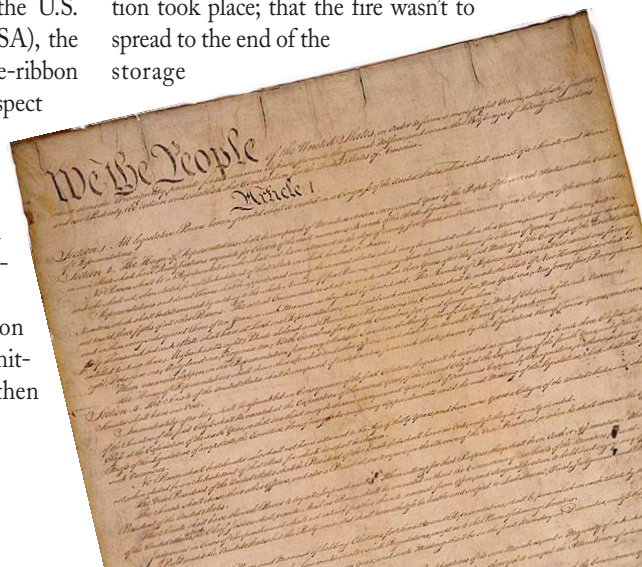
president of NFPA, was vice chair. The committee included representatives from the Public Building Service, the Society of Fire Protection Engineers, Factory Mutual Research Corporation, the Society of American Archivists, the American Institute of Architects, the American Historical Association, the International Association of Fire Chiefs, the American Library Association, the Association of Records Managers and Administrators, and the Fire Marshals Association of North America.

The fire tests

As a result of the committee's findings and the Comptroller General's 1974 report on the fire and on the status of fire protection at the other GSA records centers, the U.S. House of Representatives Committee on Government Operations authorized a series of fire tests of paper records storage. Three large-scale fire tests were conducted in 1974 by the Factory Mutual Research Corporation at the FM Test Center in West Gloucester, Rhode Island.

The object of these tests was to determine the effectiveness of standard 1/2-inch (1.2-centimeter) orifice, 280°F (133°C) rated automatic sprinklers on 10-foot-by-10-foot (3-meter-by-3-meter) spacing with a water supply discharge rate of 0.30 gallons per minute (gpm) per square foot [1.1 liter per minute (lpm) per square meter]. The storage arrangement was the government-standard shelving array, 14 shelves high, with 6 cubic feet (0.17 cubic meters) of records on each shelf. The shelving units were laid out back-to-back, and a catwalk was added above the middle layer of shelving for the final test.

The fire control criteria, which were satisfied in all tests, stated that the fire wasn't to spread across any aisle but the one where ignition took place; that the fire wasn't to spread to the end of the storage



segment; and that the fire was not to activate more than 25 sprinklers.

In 1978, NARA began fire testing record storage in mobile or "compact" steel shelving systems, as well. Factory Mutual again conducted three full-scale fire tests using the same sprinkler design as in 1974.

While this protection system was adequate to protect the building, NARA determined that it didn't meet its goal of limiting the loss of records.

In 1980, Factory Mutual conducted three additional fire tests for NARA. While the shelving configuration remained the same, this test series used large-drop sprinklers, temperature rated at 280°F (133°C) and installed on a 10-foot-by-10-foot (3-meter-by-3-meter) spacing. Water pressure was kept constant at 25 pounds per square inch (11 kilograms per square centimeter), producing a discharge rate of approximately 56 gpm (211 lpm) per sprinkler. The catwalk was again installed for the third test.

All three tests demonstrated that the large-drop sprinkler system controlled the fire and limited fire damage to a small area around the ignition point. In the third test, fire control remained excellent, but the system provided only marginal protection for exposed structural steel.

In 1989, NARA commissioned two more full-scale fire tests of mobile shelving systems. This time, Underwriters Laboratories (UL) of Northbrook, Illinois, conducted the tests.

The sprinkler system used standard-orifice, quick-response upright sprinklers on a 10-foot-by-10-foot (3-meter-by-3-meter) spacing, again with a design discharge of 0.30 gpm per square foot (1.1 lpm per square meter). The sprinklers had a temperature rating of 165°F (74°C) and incorporated quick-response-type heat-responsive elements with a response time index of approximately 50 (feet-seconds)^{1/2} (15 (meters-seconds)^{1/2}).

The controls for the electric motor-driven shelving unit were modified, allowing the rows to shift automatically to reduce the spacing between adjacent rows a uniform 4 to 5 inches (10 to 12 centimeters) in the early stages of a fire, following activation of a smoke detector.

In both tests, the systems controlled the fire effectively, limiting damage primarily to two rows exposed to the incipient fire.

In 1996, UL conducted two more tests. This time, another shelving layer was added to make the array of shelves eight high, and the temperature rating was dropped to 155°F (68°C). In the second test, the system design density was reduced to 0.20 gpm per square foot (0.75 lpm per square meter). Both these tests were successful.

Three years later, NARA returned to live fire testing, this time at the Southwest Research Institute in San Antonio, Texas. The ignition scenario in this series used a simulated box fire at the base of the shelving unit to one side of the aisle.

Researchers used a shelving array 30 feet, 8 inches (9 meters, 20 centimeters) tall with units connected by catwalks at 16 feet, 3

EVEN THE BEST DESIGNED SYSTEMS CAN FAIL OR BE PREVENTED FROM OPERATING.

inches (5 meters, 7 centimeters) and at 24 feet, 6 inches (7 meters, 15 centimeters).

Sprinklers were installed under the catwalks at the center of the aisle 15 feet, 7 inches (4 meters, 17 centimeters) above the finished floor and 23 feet, 10 inches (7 meters, 25 centimeters) above the finished floor on 7-foot (2-meter) centers. The upper level was offset 3 feet, 6 inches (0.91 meters, 15 centimeters).

The under-catwalk sprinkler system consisted of quick-response sprinklers with 1/2-inch (1.2-centimeter) orifices rated at 155°F (68°C). They could deliver a 25-gpm (95-lpm) flow and had 4 1/2-inch (11-centimeter) heat collectors/fork-lift guards. The ceiling sprinklers, which were installed on a 10-foot-by-10-foot (3-meter-by-3-meter) spacing, were rated at 286°F (141°C) and had 0.53-inch (1.3 centimeter) orifices. This test demonstrated effective fire control.

Implementing the test results

The fire tests and NARA's real-world experi-

ence have led to the development of comprehensive fire protection systems for federal records storage facilities across the country, based on the requirements of a well-defined set of fire protection standards, many of which reference NFPA documents. Among the NFPA documents NARA incorporates by reference in its records center facility standards are NFPA 10, *Portable Fire Extinguishers*; NFPA 13, *Installation of Sprinkler Systems*; NFPA 20, *Installation of Stationary Pumps for Fire Protection*; NFPA 72, *National Fire Alarm Code*®; NFPA 101®, *Life Safety Code*®; NFPA 221, *Fire Walls and Fire Barrier Walls*; and NFPA 232, *Protection of Records*. Although not cited in its facility requirements, NARA also uses NFPA 2001, *Clean Agent Extinguishing Systems*, for high-value collections.

Specifically, NARA regulations require that all records storage and adjoining areas be protected by a professionally designed fire-safety detection system and protected by a suppression system designed to limit the maximum anticipated fire loss to 300 cubic feet (8.4 cubic meters) of records.

In addition to the automatic sprinkler designs, an essential component of the protection system is the shelving. A solid steel shelf supports each layer of boxes, which nominally measure 1 cubic foot (0.0283 cubic meter). The shelves delay the spread of fire vertically and prevent boxes from falling into the aisles. In tests in which several layers of boxed records were stored on top of each other on a single shelf in traditional warehouse racks, the lower boxes failed, causing the upper boxes to cascade into the aisle, contributing to rapid fire development.

Since even the best designed systems can fail or be prevented from operating, NARA limits the number of federal records stored in a single fire compartment to 250,000 cubic feet (7,079 cubic meters) of records.

Because arson is a leading cause of records center fires, physical and personnel security are also important components of NARA's protection system. Access to record storage areas is strictly controlled, and the facilities are under electronic surveillance at all times. 🔥

(The views expressed in this article are those of the author and do not necessarily represent NARA's.)

How NFPA 232 Can Help You Protect Your Records

NFPA 232 defines a vital record and how to protect it.

■ DAVID R. HAGUE

THE MAINTENANCE AND STORAGE of information, be it on paper or magnetic media in highly protected controlled atmospheres or valuable office space, can be time-consuming and costly. However, the loss of records can be devastating, producing serious cultural and historical effects, as well as legal and business implications.

How can we determine what information should be preserved and prevent its loss? NFPA 232, *Protection of Records*, can help.

Introduced in 1947, NFPA 232 was one result of the 1922 Chicago, Burlington, and Quincy Railway office building fire in Chicago, which destroyed every

record of the physical valuation of the railroad's properties, a loss reported to have cost the company \$7.5 million in 1922 dollars. (See "Looking Back" on page 96.) This fire showed that valuable and irreplaceable records, even when stored in a so-called fire-resistant building, could be lost forever unless properly protected.

Now in its 11th edition, NFPA 232 contains requirements and guidance valuable for protecting paper records and magnetic media, and covers such topics as emergency planning, fire risk evaluation, and operations and housekeeping issues. The only topics it doesn't address are the protection of cellulose nitrate film records and forcible entry.

Unlike other standards, such as NFPA 13, *Installation of Sprinkler Systems*, which can be mandated by building codes or local codes and ordinances, compliance with NFPA 232 is mandated by the owner of the record, whom the standard refers to as "the responsible party," since he or she is the only one who can determine the record's value. How does the responsible party do this? Primarily by answering the question, "Would the loss of this record cause a serious legal or business impairment?" The answer will determine the level of protection necessary, something only the responsible party can do.

As defined by NFPA 232, a record is considered "vital" if it's irreplaceable and contains information that would cause a serious legal problem or business interruption if it were unavailable, even temporarily. Financial records or artifacts are usually considered vital records. An "important" record is one for which a reproduction can substitute for the original but only at considerable expense or delay. And the loss of a "useful" record might cause temporary inconvenience, but it may not result in a serious disad-

vantage. Each type of record requires different levels of protection (see Table 1).

Once the responsible party has determined the level of protection needed, he or she can consult NFPA 232 for the construction and fire protection requirements for each type of storage facility or device. Let's begin with the highest level of protection, a vault.

A regular records vault is limited to a total volume of 5,000 cubic feet (141 cubic meters), with a maximum interior height of 12 feet (4 meters). Should the quantity of records exceed this volume, an oversized records vault, no larger than 25,000 cubic feet (708 cubic meters), can be built. Unlike a regular records vault, however, an oversized vault must be equipped with an automatic suppression system in accordance with NFPA 13; NFPA 750, *Water Mist Fire Protection Systems*; or NFPA 2001, *Clean Agent Fire Extinguishing Systems*. Refer to the appropriate tables in NFPA 232 to determine the fire-resistance rating for both types of vaults, depending on the fire-resistance rating of the building. This rating can be as long as six hours.

To provide the highest level of protection possible, vaults must be supervised during working hours, and access must be limited to authorized personnel. Vaults can't be used as working spaces.

A file room provides the next level of protection and is used to store important, long-term temporary or permanent records only. Vital records should never be stored in a file room (see Table 1).

A file room is limited to 50,000 cubic feet (1,416 cubic meters) of total volume. It must be equipped with an automatic sprinkler system, although the sprinkler system can be omitted if all the records in the room are stored in six-sided, noncombustible containers. A six-sided container is necessary to avoid records exposure as opposed to an open box. As with vaults, the fire-resistance rating of a file room must comply with the information found in Table 2 or 3 of NFPA 232. This rating can be as much as six hours.

Like a vault, a file room must be supervised during working hours and inspected daily to ensure that all records are stored



in their containers, wastepaper is removed, and the room is locked when closed. Records in a file room must be stored at least 3 inches (8 centimeters) above the floor to prevent water damage.

Access to a file room must be limited to individuals authorized to handle the records. However, the room can be used as a working space, since it's either protected by an automatic sprinkler system or the records are stored in six-sided, noncombustible containers. Because the storage volume of, and access to, file rooms are limited and they're protected by automatic sprinkler systems, they offer a high level of protection for records.

If you have a small quantity of vital records and a vault isn't practical, you may store them in a fire-resistant safe or an insulated records container, filing device, or drawer. Regardless of the protection equipment you choose, you must make sure it's rated, and you must select the rating from tables in NFPA 232.

Storage devices

The choice of storage device classification should be based on the type of media stored. Storage devices are classified in accordance with UL 72, *Standard for Tests for Fire Resistance of Records Protection Equipment*, which evaluates them using interior temperature and relative humidity limits over a period of time.

The limit for computer disks is 125°F

(52°C) with 80 percent relative humidity, while the limit for photographic, magnetic, or other non-paper records is 150°F (65.5°C) with 85 percent relative humidity. For paper records, the limit is 350°F (196°C) with 100 percent relative humidity. Storage device time limits are classified from one to four hours.

Long-term, temporary, and permanent records are generally stored in records centers, which must be of noncombustible construction and equipped with an automatic sprinkler system. Currently, records centers' maximum storage volume is limited to 250,000 cubic feet (7,079 cubic meters) per compartment, and fire walls separating compartments must be built of four-hour, fire-resistive construction.

Permanent records that are typically stored in archives are subject to the same construction requirements as records centers. However, archives are limited to a maximum storage volume of 125,000 cubic feet (3,540 cubic meters).

Emergency plans

Regardless of the type of record stored or the level of protection chosen, no records protection strategy is complete without an emergency plan. Chapter 6 of NFPA 232 provides requirements and guidance for establishing such a plan.

The responsible party should appoint a risk manager who's responsible for protecting the site. In addition to overseeing the life

safety systems; fire prevention, inspection, and property surveys; and the proper operation and maintenance of the fire protection equipment, the risk manager should also develop and implement an emergency plan. This plan should include an annual exercise involving both management and staff, and lessons learned from the exercise should be used to update the plan.

So how can you protect your business records? For small quantities of most private and business records, a rated storage device will suffice. For medium-sized collections, however, a dedicated storage space constructed and protected in accordance with NFPA 232 is essential. For even larger collections, a commercial records storage firm is needed.

Regardless of the way you choose to store your records, you should follow NFPA 232's guidelines for the best protection and preservation method. 🔥

Stephen E. Hannestad is chairman of the NFPA 232, *Protection of Records*, technical committee and director of the Acquisitions and Systems Management Division for the U.S. National Archives and Records Administration.

Scott Baltic is a Chicago-based freelance writer and former editor of *Fire Chief* magazine.

David R. Hague is a senior fire protection engineer at NFPA and serves as staff liaison to NFPA 232.

TABLE 1

Record Type	Vault	Archive	Records Center	File Room	Storage Device
Important				X	
Intermediate-term ¹					
Long-term			X	X	
Temporary			X	X	
Permanent	X	X	X	X	
Sample/Select ¹					
Unscheduled ¹					
Useful ¹					
Vital	X				X

¹Protection should be in accordance with NFPA 13, *Installation of Sprinkler Systems*, and NFPA 230, *Fire Protection of Storage*.