

Risk Analysis and Control: Vital to Records Protection

Identifying and preventing risk is smart business practice. This excerpt from *Records and Information Management: Fundamentals of Professional Practice* gives the fundamentals of assessing risk in your records operations, putting a prevention plan in place, and auditing that plan for compliance.

William Saffady, Ph.D.

Risk analysis determines and evaluates the exposure of vital records to specific risks. Its outcome provides the basis for protection planning and other records management decisions. A thorough risk analysis begins with the identification of threats and vulnerabilities to which vital records are exposed. Once identified, threats and vulnerabilities can be evaluated using qualitative or quantitative approaches. Risk control is also an important component of any vital records program. The purpose of risk control is to safeguard vital records. Where vital records protection is part of a broader business continuity and disaster recovery plan, risk control measures may also safeguard facilities, computer hardware and software, laboratory equipment, and other resources.

Identifying Risks

Threats to vital records are customar-

ily divided into three broad categories: (1) destruction, (2) loss, and (3) corruption. A fourth category – threats associated with the improper disclosure of recorded information – is typically outside the scope of records management responsibility.

Protection of essential information against malicious or accidental destruction is a well-established component of vital records planning. Malicious

destruction of recorded information may result from warfare or warfare-related issues. Potentially catastrophic agents of accidental destruction include natural disasters. Vital records can also be damaged or destroyed by human-induced accidents such as fire or lack of knowledge about the consequences of specific actions.

More likely causes of accidental records destruction are less dramatic and more localized but no less catastrophic in their consequences for mission-critical operations. Records in all formats can be damaged by careless handling. Paper documents, for example, are easily torn, damaged by spilled fluids, or otherwise mutilated. Microforms, X-rays, and other photographic films can be scratched. With very active records, the potential for such damage is intensified by use. In many work environments, for example, valuable engineering drawings subject to frequent retrieval are characteristically frayed and dog-eared.

At the Core

This article

- ▶ Looks at the qualitative and quantitative approaches to risk analysis
- ▶ Reviews preventative and protective measures of control
- ▶ Discusses the importance of a compliance auditing program

Information recorded on magnetic media and certain types of optical disks can be erased by exposure to strong magnetic fields. Careless work procedures, such as mounting magnetic tapes or diskettes without write protection, can expose vital electronic records to accidental erasure by overwriting. Mislabeled rewritable media may be inadvertently marked for reuse, their contents being inappropriately replaced by new information. Computer hardware and software failures can damage valuable information. Electronic records may be accidentally deleted during database reorganizations or by utility programs that consolidate disk space.

Records in all formats can be misfiled, misplaced, or stolen. Like many business tasks, filing of paper records is subject to errors. Documents can be placed into the wrong folders, and folders can be placed into the wrong drawers or cabinets. Widely quoted sources claim misfile rates ranging from one to ten percent for documents in office files, but such claims are typically substantiated by anecdotal reports rather than scientific studies that present detailed statistical data about filing activity in specific work environments. Nonetheless, even a very low misfiling rate can pose significant problems in large filing installations. In a central filing area with 25 four-drawer cabinets, for example, a misfiling rate of just one-half of one percent means that more than 1,000 records are filed incorrectly. Of course, even a single misfiled document can have serious consequences if it contains information needed for an important business purpose.

Color-coded folders can simplify detection of misplaced folders, but they are not applicable to every filing situation nor can they identify individual documents filed in the wrong folder. Microfilm's advocates claim that it will eliminate misfiles associated with refiling activity. However, unless misfile detection is performed during document preparation, pages can be microfilmed in the wrong sequence, in which case misfiles are irreversible. Further, individual micro-

fiche, microfilm jackets, and aperture cards can themselves be misfiled within cabinets or trays. With electronic records, data entry errors are the counterparts of

Tampering is a leading cause of corruption of recorded information, but not all record formats are equally vulnerable. With microforms, tampering is difficult

Trade secrets, product specifications, manufacturing methods, marketing plans, pricing strategies, and customer information are of great interest to a company's competitors.

misfiles. Although effective methods, such as double-keying of information, are available for error detection and correction, they are not incorporated into all data entry operations.

Like any valued asset, recorded information can be stolen for financial gain or other motives, by intelligence operatives or by disgruntled, compromised, or coerced employees. Traditionally, espionage-related concerns have been most closely associated with government and military records, but they apply to other work environments as well. Commercial information brokers, for example, are interested in names, addresses, telephone numbers, and other information about an organization's employees, a company's customers, a hospital's patients, an academic institution's students, and a professional association's members. Trade secrets, product specifications, manufacturing methods, marketing plans, pricing strategies, and customer information are of great interest to a company's competitors.

The threat of theft is greatest for records stored in users' work areas where systematic handling procedures are seldom implemented and security provisions may be weak or absent. Centralized repositories, by contrast, tend to be more secure. Theft is a concern for records in all formats; but microforms and electronic media are compact and more easily concealed than paper documents, and their high storage densities increase the amount of information affected by a single incident of theft.

and detectable. The contents of individual microimages cannot be altered, and insertion or removal of images requires splicing of film, which is readily apparent. By contrast, information in paper documents can be added to, obliterated, or changed, although such modifications can often be detected by skilled forensic examiners. The potential for unauthorized tampering with electronic records has been widely discussed in publications and at professional meetings. Records stored on rewritable media—such as magnetic disks, magnetic tapes, and certain optical disks—are subject to modification by unauthorized persons in a manner that can prove very difficult to detect. Such unauthorized modification may involve the deletion, editing, or replacement of information. Further, viruses and other malicious software can damage computer-stored records.

Qualitative Risk Assessment

Regardless of the specific threats involved, risk assessment may be based on intuitive, relatively informal qualitative approaches or on more structured, formalized quantitative methods. The methods are not mutually exclusive; they can be used in combination to evaluate the risks to which specific vital records are subject and to produce a prioritized list of vital records for which protective measures are recommended.

Qualitative risk assessment is the simpler of the two approaches. It relies principally on group discussions involving

Risk Assessment Formula

R = P x C

where:

R = the risk associated with the loss of a specific vital records series due to a catastrophic event or other threat

P = the probability that such a threat will occur in any given year

C = the cost of the loss if the threat occurs

knowledgeable persons. Qualitative risk assessment is particularly useful for identifying and categorizing physical security problems and other vulnerabilities. A risk assessment team or committee, preferably led by a records manager, identifies and evaluates the dangers to specific vital records series from catastrophic events, theft, misfiling, or other threats.

A qualitative risk assessment is usually based on a physical survey of locations where vital records are stored, combined with a review of security procedures already in place. Among items the risk assessment team may consider are geophysical and political factors, reported problems with destruction or loss of records, number and types of employees who have access to records, records handling procedures that may result in damage to or loss of records, physical security, building construction, and access controls in records storage areas, the proximity of records storage areas to laboratories, factories, or other facilities that contain flammable materials or hazardous substances, availability of fire control apparatus and fire department services, and ability to reconstruct recorded information through backup procedures or other methods.

Although the nature and frequency of destructive weather, misfiles, theft of records, or other adverse events are examined and evaluated, qualitative risk assessments do not estimate their statistical probabilities or the financial impact of resulting losses. Instead, consequences and probabilities are evaluated in general terms. Consequences associated with the loss of specific records series, for example, may be categorized as devastating, serious,

limited, or negligible. Similarly, the likelihood of significant information loss associated with specific threats may be described as very low, low, medium, high, or very high.

In the project team's assessment, these evaluative designations should be accompanied by definitions or a clarifying narrative. The greatest concern is for vital records with high exposure to threats that have a high probability of occurrence with sudden, unpredictable onset – for example, researchers' notebooks stored in laboratory areas where flammable chemicals are routinely used in scientific experiments, or confidential product specifications and pricing information stored in file cabinets or left on desktops in unsecured office areas.

Quantitative Risk Assessment

Quantitative risk assessment is based on concepts and methods originally developed for product safety analysis and subsequently adapted for computer security applications. Like its qualitative counterpart, quantitative risk assessment relies on site visits, discussions, and other systems analysis methodologies to identify risks, but it uses numeric calculations to estimate the likelihood and impact of losses associated with specific vital records series. The losses are expressed as dollar amounts, which can be related to the cost of proposed protection methods. Compared with qualitative methods, quantitative risk assessment provides a more structured framework for comparing exposures for different vital records series and prioritizing vital records protection recommendations.

Although various quantitative assess-

ment techniques have been proposed by risk analysts and others, all are based on the general risk assessment formula.

The risk assessment formula measures risk, sometimes called the annualized loss expectancy (ALE), as the probable annual dollar loss associated with a specific vital records series. The total expected annual loss to an organization is the sum of the expected annualized losses calculated for each vital records series.

Quantitative risk assessment begins with the determination of probabilities associated with specific events and the calculation of annualized loss multipliers based on those probabilities. Quantitative risk assessment has a subjective component in so far as the qualitative risk assessment approach is typically used to determine the probabilities. Program unit personnel or others familiar with a given records series are asked to estimate the likelihood of occurrence for specific threats. Whenever possible, their estimates should be based on the historical incidence of adverse events, which can be accurately determined in some cases but only approximated in others. Reliable frequency information is easiest and most conveniently obtained for incidents such as burglaries, fires, power outages, equipment malfunctions, software failures, network security breaches, and virus attacks for which security reports, maintenance statistics, or other documentation exists. The frequency of potentially destructive geophysical or political events, such as hurricanes or terrorist attacks, may likewise be documented in books, newspapers, or other published sources.

In the absence of written evidence or experience, probability estimates must be based on informed speculation by persons familiar with the circumstances in which a given vital records series is maintained and used. Often, a records manager must ask a series of probing questions, followed by lengthy discussion, to obtain usable probability estimates. As an example, the records manager may ask employees of a human resources department whether the inability to locate essential personnel files is likely to occur once a year. If the answer

Preventive Risk Control Measures

The following preventive risk control measures promote the physical security of vital records against malicious destruction or unauthorized access

- One storage location is easier to secure than many. In this respect, centralized records repositories are preferable to decentralized ones. Where vital records are maintained in user areas, security is difficult to enforce and easily compromised.
- Access to vital records storage areas should be limited to a single supervised entrance. Other doors should be configured as emergency exits with strike bars and audible alarms.
- Access should be restricted to authorized individuals who have a specific business reason for entering such areas. Badges should identify authorized individuals.
- Employees should be instructed to challenge and report suspect persons who enter vital records repositories.
- All containers should be examined on entry into or removal from the vital records repository.
- Janitorial services in the vital records repository must be performed in the presence of authorized employees.
- Areas where vital records are stored or used should never be included in building tours.
- Vital records should be filed in locked drawers, cabinets, or other metal containers until needed and returned to their filing locations immediately after use.
- A "clean desk" policy is recommended. Vital records must never be left unattended on work surfaces, and all vital records must be put away at the end of the workday.
- Confidential personal data, trade secrets, or other sensitive information should not be stored in mobile computing devices, which are easily stolen. If using mobile devices is unavoidable, they must never be left unattended.
- Vital electronic records stored on networked computers can be accessed, and possibly damaged, by remote users. Physical security measures must consequently be supplemented by safeguards against electronic intrusion.
- Access to vital electronic records and their associated software should be controlled by passwords or personal identification numbers.
- Access to computer workstations must be restricted to authorized employees. Computer workstations should be turned off—and locked, if possible—when not in use. They should never be left unattended while operational. System software should automatically terminate a computer session after a predetermined period of inactivity.
- Mission-critical applications and vital electronic records should be isolated from publicly accessible computer resources in organizations connected to the Internet.

is yes, the records manager should ask whether such an event is likely to occur once every half year, once a quarter, once a month, and so on. This procedure can be repeated until a satisfactorily specific response is obtained.

Once probabilities are estimated, annual loss multipliers can be calculated in any of several ways. Using one method, a calamitous threat to vital records with a given probability of occurrence is assigned a probability value of 1. Other threats are assigned higher or lower values, based on their relative probability of occurrence.

Applying the formula given previously, the probability value is multiplied by the estimated cost of the loss if the event occurs. Factors that might be considered when determining costs associated with the loss of vital records include, but are by no means limited to, the following:

- The cost of file reconstruction, assuming that reconstruction is possible
- The value of canceled customer orders, unbillable accounts, or other business losses resulting from the inability to perform specific business operations because needed records are unavailable
- The cost of defending against or otherwise settling legal actions associated with the loss of vital records

Quantitative risk assessment is an aid to judgment not a substitute for it. The risk assessment formula is an analytical tool that can help records managers clarify their thinking and define protection priorities for vital records.

Risk Control

Some recorded information may be reconstructable in the event of a disaster, but the high cost of such reconstruction makes it a last-resort component of risk control. Prevention is the first line of defense against risk. Preventive measures are designed to minimize the likelihood of damage to vital records from one or more of the threats enumerated in the preceding discussion. Preventive measures apply to

both working copies and security copies of vital records. By contrast, protective measures typically apply only to security copies, sometimes described as backup copies, of vital records. Protective measures permit the reconstruction of essential information and the restoration of business operations if one or more vital records series is destroyed, damaged, or lost.

Whether prevention or protection is involved, risk control begins with heightened security awareness formalized in organizational policy and procedures, which must be communicated to every employee who works with vital records. Information security should be the responsibility of every employee. A directive from senior management to line managers or other key personnel in individual program units should acknowledge the mission-critical importance of vital records and emphasize the need to safeguard them. Risk control guidelines should be conspicuously posted in areas where vital records are stored or used. One person in each program unit should be assigned specific responsibility for the implementation of risk control guidelines. Ideally, that person will also serve as the program unit's records management liaison. Program unit managers should be instructed to review risk control policies and procedures at staff meetings. The records manager should be available as a resource person to address such meetings and clarify risk control policies and procedures. To publicize the vital records initiative, the records manager can prepare articles on vital records and the importance of risk control for employee newsletters, intranet web pages, or other in-house publications.

Preventive Measures

Preventive risk control measures address the physical environment where vital records are stored and used. To the greatest extent possible, storage facilities for vital records should be located in areas where floods and destructive weather are unlikely. Locations near chemical factories, utility plants, airport landing patterns, and other potential haz-

ards should also be avoided. Vital records repositories should be situated away from high-traffic locations, preferably in buildings or portions of buildings without windows. Often, records managers have little control over the geographic locations where working copies of vital records are maintained, but they can specify storage locations for backup

copies. Storage areas for vital records must be properly constructed and include appropriate smoke detection and fire-extinguishing equipment.

Protective Measures

Protective measures permit the reconstruction of vital records to support the restoration of mission-critical operations

in the event of a disaster. Such measures have historically relied on specially designed storage enclosures and purposeful duplication of records for offsite

mined intervals is routine operating procedure in most mainframe and mini-computer installations and for information stored on network servers. However,

For effective vital records protection, backup responsibilities must be clearly delineated. Backup schedules must be established and rigidly enforced.

storage. These measures are most effective when combined.

Specially designed filing cabinets, vaults, and other storage enclosures provide onsite protection of vital records against certain threats. Vital records can be protected against theft, for example, by storing them in locked file cabinets, safes, or other containers, although simple keylocks offer little resistance to a skilled intruder. Containers with high-security keylocks or combination locks are preferable.

Underwriters' Laboratories rates file cabinets, safes, and other containers for their resistance to break-in by prying, drilling, chiseling, hammering, sawing, or other means. Although tamperproof and fire-resistant storage containers can prove useful in certain situations, the most effective approach to vital records protection involves the purposeful preparation of backup copies for storage at a secure offsite location. Microfilming is usually the best practice for production of backup copies of vital paper records. Compared to full-size photocopies, microfilm copies are usually faster and cheaper to produce, and they require less storage space at the offsite location, which is an important consideration where backup copies will be housed in a commercial records center that charges by the amount of space consumed. When records are microfilmed for retention purposes, additional backup copies can be produced at a small incremental cost.

The production of backup copies of essential electronic records at predeter-

mined intervals is routine operating procedure in most mainframe and mini-computer installations and for information stored on network servers. However, backup operations may be performed sporadically, if at all, in desktop computer installations where procedures are typically less routinized and users may be unaware of the need for backup copies. For effective vital records protection, backup responsibilities must be clearly delineated. Backup schedules must be established and rigidly enforced.

Off-site storage repositories for vital records may be established and operated by a business, government agency, or other organization on its own behalf. Alternatively, a commercial records center or data vault may be utilized for offsite storage. In either case, the offsite facility must be secure.

Backup copies of vital records must be stored at a sufficient distance from the working copies so that they are unaffected by the same natural disasters or destructive events. The storage facility must be close enough, however, for convenient delivery of vital records as well as timely retrieval of backup copies to support disaster recovery. For pickup and delivery of records, some in-house and commercial storage facilities offer courier services equipped with environmentally controlled trucks or vans. Some facilities also

support electronic vaulting in which backup copies of vital electronic records are transmitted to off-site storage over high-speed telecommunications facilities.

The typical vital records repository has suitable storage facilities for paper documents, microforms, and electronic media, although some data vaults exclude paper records to minimize the danger of fire. Environmental specifications appropriate to the type of media being stored and the retention period for recorded information must be observed. Backup electrical generators should be available to maintain environmental controls in the event of power outages.

Auditing for Compliance

Once vital records are identified and appropriate loss control methods specified, the implementation of preventive and protective measures for designated records series will usually be the responsibility of personnel in the program unit that maintains the records. Periodic audits should be performed to confirm compliance. Such audits may be conducted by records management staff or delegated to another organizational unit, such as an internal audit department, that has other compliance-oriented responsibilities. In such cases, auditing for vital records compliance can be coordinated with financial or other auditing activities, thereby simplifying the scheduling of audits as well as saving both time and labor. Internal auditors can report the results of vital records compliance audits to the records manager for follow-up and corrective action where indicated. To gain the attention of top management, the internal audit reports should also be distributed to those persons who receive reports of important financial audits. ■

William Saffady, Ph.D., is a Professor at the Palmer School of Library and Information Science, Long Island University, where he teaches courses on information management topics. He is the author of more than three dozen books, including Records and Information Management: Fundamentals of Professional Practice.

Records and Information Management: Fundamentals of Professional Practice is available from the ARMA International Bookstore (www.arma.org/bookstore).