©2015 ARMA International

As an important part of vital records planning, records managers must consider the risks to which specific record series are subject. The purpose of risk analysis, sometimes termed risk assessment, is to determine and evaluate exposure to particular risks. Its outcome provides the basis for protection planning and other records management decisions.

The following discussion is based on the common business definition of *operational risk* as a danger of damage or loss to an organization resulting from inadequate internal processes, including inadequate information management practices, or from external events.

This definition, which was originally developed for the banking industry, has since been widely applied to other types of organizations. The definition encompasses legal risks resulting from failure to comply with laws, regulations, or contractual obligations.

Operational risk is a function of three variables:

1. Threats or hazards that may harm an organization
2. Vulnerabilities that render an organization susceptible to threats
3. Consequences or negative impacts associated with specific threats

The next section surveys threats and vulnerabilities that an organization must consider when developing a program to protect vital records.

Threats and Vulnerabilities

Vital records may be threatened by loss or damage from a variety of causes. For example:

Malicious Destruction of Recorded Information

This loss may result from warfare or warfare-related activities such as terrorist attacks and civil insurrections. Vital records are also subject to purposeful sabotage or seemingly aimless vandalism by current or former employees, contractors, intruders, or others. An organization's vulnerability to these threats depends on various factors, including the na-

Count the Cost: **Quantifying Your Vital Records' Risks**

William Saffady, Ph.D., FAI

Quantitative risks assessment, which uses numeric calculations to measure the likelihood and impact of the loss of specific vital records, provides a solid basis for planning how to protect them.

©2015 ARMA International

ture of the organization's business, the local socio-political environment, proximity to sites that are subject to terrorist attack or armed conflict, and security provisions in place.

Accidental Destruction

Potentially catastrophic agents of accidental destruction include natural disasters, such as violent weather, floods, earthquakes, landslides, and volcanic eruptions as well as fires, explosions, building collapses, and other events that may result from carelessness, negligence, or lack of knowledge about the consequences of specific actions.

An organization's vulnerability to these disastrous events depends on geographical, geological, and meteorological factors that may be unpredictable and unpreventable. Vulnerability is obviously increased by close proximity to factories or laboratories that manufacture or utilize flammable materials, airports, military bases, power plants, refineries, storage facilities for oil or natural gas, and major highways and railway lines that are used for transport of hazardous materials. Vital records can also be damaged or destroyed by fire. Vulnerability is increased in rural locations that are remote from firefighting services.

Careless Handling

More likely causes of accidental record 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.

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.

Information recorded on magnetic media and certain optical disks can be erased by exposure to strong magnetic fields. Careless work procedures, such as mounting tapes or disks without write protection, can expose vital records to accidental erasure by overwriting.

> . . . systemic procedures for media storage, care, and handling can reduce an organization's vulnerability to these threats

Mislabeled media may be inadvertently marked for reuse, their contents being inappropriately replaced by new information. The implementation of systematic procedures for media storage, care, and handling can reduce an organization's vulnerability to these threats.

Misfiled Records

Records in all formats can be misplaced. Like many business tasks, filing of paper records is subject to errors. Even a very low misfiling rate can pose significant problems in large filing installations. In a central filing area with 25 four-drawer cabinets totaling 200,000 to 250,000 pages, for example, a misfiling rate of just one-half of one percent means that over 1,000 pages are filed incorrectly. Of course, even a single misfiled document can have serious consequences if it contains information needed for an important business purpose.

In digital document management implementations that use computer-based indexing, data entry errors are the counterparts of misfiles. While effective methods, such as double-keying of information, are available for error detection and correction, they are not incorporated into all data entry operations.

Stolen Recorded Information

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, Social Security 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.

Burglars, confidence artists, and other criminals are interested in financial and asset information contained in donor and patron records maintained by charitable and cultural institutions. A museum's records, for example, indicate the owners and locations of valuable art works. A university development office's files contain addresses and possibly financial data about prospective benefactors.

The use of compact, easily concealed storage media – such as high-density magnetic tapes, solid-state memory devices, optical disks, and microforms – facilitates theft, while the high capacity of such media increases the amount of information affected by a single incident of theft.

Computer Hardware and Software Failures

These types of failures can damage

©2015 ARMA International

valuable information. Head crashes or other hardware malfunctions, while much less common than in the past, can destroy valuable information recorded on hard drives. Improperly adjusted equipment, such as misaligned tape guides, can cause scratches or other media damage.

An organization can minimize its vulnerability to these problems by keeping its computer hardware in good working order and replacing aging equipment, but hardware malfunctions cannot be eliminated completely.

Software failures are more difficult to control. When a computer program locks up or terminates abnormally, information may not be properly recorded. Similarly, computer records may be accidentally deleted during database reorganizations or by utility programs that consolidate space on hard drives. Viruses and other malicious software are much publicized causes of corruption of computer-stored records.

Tampering

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

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. Password protection, encryption, and other countermeasures can reduce but not entirely eliminate an organization's vulnerability to such data tampering.

If the calculated cost of a given loss exceeds the cost of protective measures, those measures should be implemented

Improper Disclosure of Recorded Information

Whether accidental or intentional, improper disclosure of recorded information has been the subject of considerable discussion by a variety of interested parties, including records managers, computer specialists, lawyers, public policy analysts, and civil rights advocates. While such discussions have typically warned against the unauthorized disclosure of sensitive personal information protected by privacy legislation, an organization's records may also store business plans, pricing information, trade secrets, or other proprietary technical, strategic, or financial information of interest to competitors. Certain government agencies store records with national security implications.

Improper disclosure of vital records may result from espionage-related activities such as unauthorized access to computer systems, electronic eavesdropping, or bribery of employees who have access to desired information. Computer networks are vulnerable to intrusion by hackers.

Accidental disclosure is also possible when computer output is routed to the wrong device in a local or wide area network, when correspondence or e-mail messages are incorrectly addressed or distributed, or when incompletely erased computer media are distributed for reuse.

Quantitative Risk Assessment

Regardless of the specific threats involved, risk assessment may be based on intuitive, relatively informal qualitative approaches or more structured, formalized quantitative methods.

Quantitative risk assessment relies on site visits, discussions, and other systems analysis methods to identify vulnerabilities, but it uses numeric calculations to measure the likelihood and impact of losses associated with specific vital record series. The calculations are expressed as dollar amounts, which can be related to the cost of proposed protection methods. If the calculated cost of a given loss exceeds the cost of protective measures, those measures should be implemented.

As an additional advantage, quantitative risk assessments provide a useful framework for comparing exposures for different vital record series and prioritizing them for protection.

Risk Assessment Formula

While various quantitative assessment techniques have been proposed by risk analysts and others, all are based on the following general formula:

$R = P \times C$
where:

R = the risk, sometimes called the *annualized loss expectancy (ALE)* associated with the loss of a specific vital record series due to a catastrophic event or other threat;

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

C = the cost of the loss if the threat occurs.

©2015 ARMA International

This formula measures risk as the probable annual dollar loss associated with a specific vital electronic record series. The total annual expected loss to an organization is the sum of the annualized losses calculated for each vital electronic record series.

Probability Estimates

Quantitative risk assessment begins with the determination of probabilities associated with adverse events and the calculation of annualized loss multipliers based on those probabilities. Information systems specialists, program unit personnel, or others familiar with a given electronic record 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.

Reliable probability estimates are easiest and most conveniently obtained for events 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.

Statistical data about potentially destructive weather events, such as hurricanes or floods, is available in books, scholarly journals, newspapers, and other reference sources, including a rapidly increasing number of websites. At its website, for example, the Federal Emergency Management Agency (FEMA) will display flood hazard maps for any U.S. location. Various websites provide information about the frequency of hurricanes, tornadoes, earthquakes, landslides, volcanic eruptions, and tsunamis worldwide.

In the absence of written evidence or experience, probability estimates must be based on informed speculation by persons familiar with the broad information management environment within which a given vital record series is maintained and used.

Quantitative risk assessment begins with the determination of probabilities associated with adverse events

In this respect, quantitative risk analysis resembles the qualitative approach. Often, the 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 a file room supervisor whether lost documents are likely to be reported once a year. If the answer 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.

Annual Loss Calculations

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.

As an example, a threat estimated to occur once a year is assigned a probability value of 1, which serves as a baseline for other probability estimates. An event estimated to occur once every three months (four times a year) is assigned a probability value of 4, while an event with an estimated frequency of once every four years is assigned the probability value of 0.25.

Probability x Cost

Applying the risk assessment formula, 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 source documents or other input materials remain available.

The value of canceled customer orders, unbillable accounts, or other losses resulting from the inability to perform specific business operations because needed electronic records are unavailable.

Labor costs associated with reversion to manual operations, assuming that such reversion is possible.

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 presented earlier is an analytical tool that can help records managers clarify their thinking and define protection priorities for vital electronic records.

As an example, assume that a hospital administrator, based on previous experience, estimates one incident a year in which a patient's folder essential to mission-critical medical care is lost through misfiling – a clinician's failure to return the folder to the medical records area following treatment, or for some other reason.

A probability (P) of 1 is assigned to the risk that a patient folder will be lost in this manner. If the estimated cost (C) is $3,000 to reconstruct medical records contained in the lost folder by obtaining copies of records from physicians' offices, re-examining the patient, repeating medical

©2015 ARMA International

tests, or other means, the risk (annualized loss expectancy) is 1 times $3,000.

Again based on its experience, the hospital administrator estimates one chance in 10 years that as many as 100 patient folders will be destroyed by flood, fire, or destructive weather. A probability (P) of 0.1 is assigned to that risk, indicating that it is one-tenth as likely to occur as the loss of one patient folder a year for reasons described above, but the risk affects many more folders. If the cost (C) to reconstruct lost patient records is $3,000 per folder, the damage will total $300,000. The risk (annualized loss expectancy) is 0.1 times $150,000, or $30,000.

These calculations indicate that destruction of patient records by a catastrophic event, while having a much lower probability of occurrence, poses a more significant risk than loss of patient records by misfiling or other reasons. Consequently, the catastrophic event should be made a higher priority for vital records protection. Given these parameters, greater attention should be given to protecting records against fire, flood, or destructive weather than to implementing procedures that will prevent misfiling of patient folders.

Importance of Analyzing Risk

Whatever the threat, vital records programs provide formalized procedures to help an organization withstand and limit the impact of adverse events, enabling it to continue information-dependent business operations – though possibly at a reduced level – following a disaster.

Risk analysis to determine the extent to which specific vital records are threatened by hazards and to calculate exposures, which allows the selection of appropriate loss prevention and record protection methods, constitutes a critical component of your vital records protection program.

To learn more about analyzing risk or about a wide variety of information management topics, read the comprehensive text *Records and Information Management: Fundamentals of Professional Practice*, 2nd ed., from which this article was excerpted. **END**

William Saffady, Ph.D., FAI, can be contacted at wsaffady@aol.com. *See his bio on page 47.*