Vital Records

Vital records, as briefly defined in preceding chapters, contain information that is essential to an organization's mission. All organizations have certain business operations that they must perform. Such operations are characterized as mission-critical because they directly relate to an organization's reason for existing. A failure or inability to perform **mission-critical operations** will have an adverse impact on an organization's most important initiatives and, in extreme cases, the organization's continued viability. Vital records contain information needed for mission-critical business operations. All mission-critical business operations depend to some extent on recorded information. If a vital record is lost, damaged, destroyed, or otherwise rendered unavailable or unusable, such operations will be curtailed or discontinued, with a resulting adverse impact on the organization.

Vital records protection is one of the most important components of a systematic records management program. Recognizing this, ISO 15489-1, *Information and Documentation—Records Management—Part 1: General*, the international records management standard, includes risk assessment and protection of records among the requirements for records management operations. The importance of protecting vital records is treated in ANSI/ARMA 5, *Vital Records Programs: Identifying, Managing, and Recovering Business-Critical Records*. Vital records protection is an aspect of the broader fields of business continuity, the ability of an organization to maintain essential business operations following a disaster, and information security, which deals with the protection of information technology and assets. These fields are covered by many international standards, including ISO 22301, *Societal Security—Business Continuity Management Systems—Requirements;* ISO 22313, *Societal Security—Business Continuity Management Systems—Guidance*; ISO/PAS 22399, *Societal Security—Guideline for Incident Preparedness and Operational Continuity Management*; ISO/IEC 24762, *Information Technology—Security Techniques—Guidelines for Information and Communications Technology Disaster Recovery Services*; ISO/IEC 27000, *Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary*;

© 2016 ARMA International. Purchaser of this PDF file is entitled to print one copy for reference. Other reproductions or redistribution is prohibited.

ISO/IEC 27001, *Information Technology—Security Techniques—Information Security Management Systems—Requirements*; ISO/IEC 27002, *Information Technology—Security Techniques—Code of Practice for Information Security Controls*; ISO/IEC 27003, *Information Technology—Security Techniques—Information Security Management System Implementation Guidance*; ISO/IEC 27014, *Information Technology—Security Techniques—Governance of Information Security*; ISO/IEC 27031, *Information Technology—Security Techniques—Guidelines for Information and Communication Technology Readiness for Business Continuity*; and ISO/IEC 27040, *Information Technology—Security Techniques—Storage Security.*

Properly conceived and administered, a vital records program can make an indispensable contribution to business effectiveness. For many organizations, information contained in vital records is their most important asset. Without vital records:

- Equipment manufacturers will be unable to build, market, deliver, or repair their products.
- Pharmaceutical companies will be unable to develop, test, or prove the safety and efficacy of chemical compounds.
- Utility companies will be unable to operate and maintain their facilities.
- Local government agencies will be unable to document property ownership, determine tax assessments, evaluate zoning applications, or issue building permits.
- Hospitals and clinics will be unable to provide effective medical care.
- Social services agencies will be unable to help those in need.
- Schools and colleges will be unable to document the attendance or academic achievements of students.
- Insurance companies will be unable to determine policy coverage, collect premiums, or process claims.
- Financial institutions will be unable to document customer account balances, evaluate loan applications, or collect debts.
- Lawyers, engineers, architects, accountants, and other professionals will be unable to serve their clients.

In many cases, the loss of recorded information can have more devastating consequences for continuation of an organization's operations than the loss of physical plant, inventory, or raw materials, which are often replaceable and insured.

Vital records are considered vital specifically and exclusively for the information they contain and the relationship of that information to an organization's mission-critical operations. Vital record status is not necessarily related to other record attributes. Physical format is immaterial; vital records may be paper documents, photographic films, or electronic media. Vital records may be active or inactive, originals or copies. Vital record status is similarly independent of retention designations. Vital records need not be permanent records; some vital records may,

© 2016 ARMA International. Purchaser of this PDF file is entitled to print one copy for reference. Other reproductions or redistribution is prohibited.

in fact, be retained for brief periods of time and replaced at frequent intervals. Furthermore, some records may be considered vital for only a portion of their designated retention periods. Invoices, billing documentation, and other accounts receivable records, for example, are vital until the matters to which they pertain are paid, although they are usually retained for several years following receipt of payment for legal reasons, internal audits, or other purposes.

Specific record attributes aside, a vital records program is a set of policies and procedures for the systematic, comprehensive, and economical control of adverse consequences attributable to the loss of mission-critical information. Many businesses, government agencies, and other organizations have developed contingency plans for the protection of personnel, buildings, machinery, inventory, and other assets in the event of fire, weather-related disasters, or other unplanned calamitous events. Protection of recorded information essential to mission-critical business operations has long been recognized as an indispensable aspect of such emergency preparedness and disaster recovery initiatives. Since the 1950s, for example, U.S. laws have mandated the identification and protection of vital operating records of federal government agencies. According to 36 CFR 1223, the management of vital records must be part of each agency's plan for continuity of business operations in the event of emergencies. Similar regulations apply to protection of government records in other countries.

Various government regulations mandate protection for vital records associated with specific business activities. Among the many examples that might be cited:

1. 45 CFR 164.308, which implements the Health Insurance Portability and Accountability Act (HIPAA), requires regulated entities and their business associates to establish and implement procedures to create and maintain "retrievable exact copies" of electronic protected health information.
2. As specified in 21 CFR 211.68, pharmaceutical companies must maintain backup copies of drug manufacturing data. According to Annex 11 of Rules Governing Medicinal Products in the European Union, manufacturing data must be backed up.
3. Financial institutions insured by the FDIC are required to have organization-wide disaster recovery and business continuity plans for their computer installations. Review of financial institutions' business continuity plans is a well-established component of examinations performed by the Federal Financial Institutions Examination Council (FFIEC), which prescribes principles and standards for federal examination of financial institutions. Its examination procedures include detail questions about the development, implementation, testing, and oversight of disaster recovery policies and procedures, including provisions for data backup and offsite storage. Other regulatory bodies that require contingency plans for depository institutions include the Comptroller of the Currency, the Federal Home Loan Bank Board, the Office of Thrift Supervision, and the National Credit Union Administration.

© 2016 ARMA International. Purchaser of this PDF file is entitled to print one copy for reference. Other reproductions or redistribution is prohibited.

4. Some Middle Eastern countries specify protection requirements for vital records maintained by financial services companies. In Bahrain, banks must store copies of vital records offsite as soon as possible after they are created. In Israel, banks must be able to reconstruct information from backup copies, which must be stored at a safe distance from the original storage location. In Saudi Arabia, financial services companies must have backup arrangements to support disaster recovery. The United Arab Emirates specifies retention periods of 7 to 10 years for backup copies of certain records maintained by securities companies and insurance companies.
5. Among South American countries, Uruguay requires banks to have sufficient backup copies to reconstruct their accounting operations and financial statements.

Traditionally, records management has emphasized the protection of vital records against accidental or willful damage, destruction, or misplacement; the last of these events encompasses a spectrum of inadvertent or malicious events ranging from misfiling to theft of records. An organization may also be harmed, however, by misuse of, alteration of, or unauthorized access to vital records. In the case of computer records, these considerations have been widely discussed by public policy analysts and legal scholars, but they also apply to nonelectronic records. Protection against unauthorized or unintentional disclosure of records is maintained by various privacy statutes. Among U.S. laws, the Privacy Act of 1974 (5 U.S. Code 552A) is the best known example. Other federal statutes with privacy provisions for recorded information include the Fair Credit Billing Act (15 U.S. Code 1637); the Fair Credit Reporting Act (15 U.S. Code 1681); the Family Educational Rights and Privacy Act (20 U.S. Code 1232); the Right to Financial Privacy Act (12 U.S. Code 3401); the Financial Services Modernization Act (15 U.S. Code 6801), the Electronic Communications Privacy Act of 1986 (18 U.S. Code 1367), the Drivers Privacy Protection Act of 1994 (18 U.S. Code 2721), the National Information Infrastructure Protection Act of 1996 (18 U.S. Code 1030), and the Children's Online Privacy Protection Act of 1998 (15 U.S. Code 6501-6505). Similar privacy laws have been passed by various states. Medical records and adoption records, in particular, are subject to state-specific privacy legislation.

Other countries have privacy and data protection legislation that restricts access to recorded information. Examples include the Canadian Privacy Act and Canadian Personal Information Protection and Electronic Document Act, the various European data protection laws modeled on European Community Data Protection Directive 95/46/EC, the Australian Privacy Act, the New Zealand Privacy Act, the Israeli Protection of Privacy Law, the Japanese Act on Protection of Personal Information, the Philippines Data Privacy Act, the Singapore Personal Data Protection Act, and the Taiwan Personal Information Protection Act.

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

© 2016 ARMA International. Purchaser of this PDF file is entitled to print one copy for reference. Other reproductions or redistribution is prohibited.

reduced level—following a disaster. A vital records protection program includes the following components:

1. Formal endorsement of the program by a directive from an organization's senior management with responsibility and authority for protection of vital records assigned to the records management activity, to be coordinated, where appropriate, with related contingency planning activities.
2. Identification and enumeration of vital records.
3. Risk analysis to determine the extent to which specific vital records are threatened by hazards and to calculate exposures.
4. The selection of appropriate loss prevention and records protection methods.
5. Employee training, implementation, and compliance auditing.

These program components conform closely to the multistep process defined in ISO/IEC 27002, *Information Technology—Security Techniques—Code of Practice for Information Security Controls*. That standard emphasizes security measures to protect computer-based information assets, including databases and their associated software, but its principles and practices are broadly applicable to recorded information in all formats. The following sections explain and discuss vital records protection requirements and program work steps in greater detail.

Establishing the Program

Citizens have a reasonable expectation that government agencies will safeguard essential records.

In U.S. law, the determination of negligence is based on a straightforward principle: if precautionary measures cost less than the losses they are intended to prevent, then the precautionary measures should be taken.

Similar expectations apply to corporate shareholders, to a financial institution's customers, to an insurance company's policyholders, to a professional services firm's clients, to medical patients, to students, and to any other persons or organizations that are affected by the record-keeping practices of others. These expectations are based on the legal concept of "standard of care," which is the degree of caution that a reasonable, prudent person would exercise in a given circumstance to prevent injury to another. Failure to do so constitutes negligence.

Vital Records Protection as a Management Responsibility

While the standard of care is most often discussed in the context of medical malpractice, it is relevant for other professional disciplines, including records management. As discussed in Chapter 1, an organization's records are assets. In any organization, senior management has ultimate responsibility for protection of assets, including the formulation and implementation of risk management and business continuity plans. It follows, then, that senior management is ultimately

© 2016 ARMA International. Purchaser of this PDF file is entitled to print one copy for reference. Other reproductions or redistribution is prohibited.

responsible for the protection of records as assets. Effective leadership and decisive action by senior management can mitigate the impact of adverse events. If the destruction or misuse of vital records results in the interruption of critical business operations, senior management must accept responsibility for the ensuing financial losses or other consequences. This idea is forcefully stated in Corpus Juris Secundum, a comprehensive legal encyclopedia that presents the principles of U.S. law as derived from legislation and reported cases. According to Volume 19, Section 491, corporate officers "owe a duty to the corporation to be vigilant and to exercise ordinary or reasonable care and diligence and the utmost good faith and fidelity to conserve the corporate property; and, if a loss or depletion of assets results from their willful or negligent failure to perform their duties, or to a willful or fraudulent abuse of their trust, they are liable, provided such losses were the natural and necessary consequences of omission on their part."

Senior management's responsibility for protecting vital records is explicitly acknowledged or implied in laws and government regulations. For example:

- Within the U.S. federal government, 36 CFR 1236.12 makes agency heads responsible for protecting vital records, which are defined as records needed to meet operational responsibilities under emergency conditions or to protect the legal and financial rights of the government and those affected by government activities.
- As specified in the Federal Information Management Security Act (FISMA) of 2002 (44 U.S. Code 3541-3549), U.S. government agencies must develop information security protection "commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of (i) information collected or maintained by or on behalf of the agency and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." As defined by FISMA, information security must provide safeguards against improper destruction of information and ensure timely and reliable access to information.
- OMB Circular A-130, issued by the Office of Management and Budget, defines policies to secure information maintained by federal government agencies. While many of its provisions are concerned with privacy protection and prevention of unauthorized access to computer systems, Circular A-130 requires U.S. government agencies to ensure that "information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information."
- The Foreign Corrupt Practices Act (FCPA) of 1977 (15 U.S. Code 78dd-1) imposes significant fines and penalties for failure to preserve records and other information pertaining to certain accounting transactions and disposition of assets. Originally intended to prevent the destruction of records in order to conceal bribery or other crimes, FCPA's recordkeeping provisions apply to all domestic and foreign companies that list their securities on U.S. exchanges.

© 2016 ARMA International. Purchaser of this PDF file is entitled to print one copy for reference. Other reproductions or redistribution is prohibited.

Violations of recordkeeping provisions can be enforced or prosecuted without regard to any violation of the FCPA's anti-bribery provisions. The FCPA was amended in 1998 by the International Anti-Bribery and Fair Competition Act, which implemented provisions of the Organization for Economic Cooperation and Development's Convention on Combating Bribery of Foreign Public Officials in International Business Transactions.

Vital Records Protection as Insurance

A vital records protection program is, in effect, an insurance policy for essential information. Like any insurance policy, vital records protection can be difficult to sell to decision-makers. Vital records protection is costly and makes no direct contribution to revenues, product development, or improvement of services. It provides no benefits unless and until a disaster occurs.

Many threats to vital records have a low probability of occurrence. Senior management may consequently ignore them in favor of more pressing business concerns. The purpose of insurance, of course, is to provide protection against the adverse impact of improbable events. Insurance protection is usually unavailable for probable events. Like all insurance policies, vital records protection must be justified by the intolerable consequences that follow an improbable but adverse event.

Senior management must be made to appreciate the potential for tangible and intangible damages associated with the loss, destruction, or misuse of vital records, however unlikely that loss, destruction, or misuse may seem. Examples of such damages include, but are by no means limited to:

- Loss of customers due to inability to fulfill orders and contracts, support products, or provide services.
- Loss of revenue or disruptions of cash flow due to lack of accounts receivable records and resulting inability to reconstruct amounts to be billed to specific customers or to process payments.
- Loss of opportunity because information needed for contracts, partnerships, joint ventures, or other business agreements is unavailable.
- Fines or other penalties for failure to provide records needed for government investigations.
- Penalties for late payment of payroll or other taxes for which records are unavailable.
- Increased assessments, plus penalties and interest, following tax audits due to inadequate documentation of business expenses, depreciation, and other deductions, allowances, and tax credits.
- Delayed compliance with governmental reporting requirements for public companies.
- Lawsuits due to inability to pay employees and document pension benefits to retirees.

© 2016 ARMA International. Purchaser of this PDF file is entitled to print one copy for reference. Other reproductions or redistribution is prohibited.

- Lack of records needed for litigation or other legal proceedings.
- Inability to document insurance claims with resulting delay or reduction in settlements.
- Reduced employee productivity due to longer completion times for product development, design, testing, marketing, support, and other information-dependent business operations.
- High labor costs to reconstruct recorded information from alternative sources, assuming that reconstruction is possible.
- Tarnished reputation and loss of customer good will.

Further, an organization may be sued for damages resulting from its failure to protect essential operating records from accidental or willful loss or destruction. A hospital's failure to protect medical records, for example, could complicate treatment and damage a patient's health. A university's failure to protect academic transcripts could place its graduates at a disadvantage when competing for employment or seeking further education. An organization's failure to protect its personnel records could result in incorrect determination of retirement eligibility or calculation of pension benefits. Loss of revenue resulting from a public company's failure to protect essential business records could lower the value of the company's stock, provoking shareholder lawsuits. Destruction of birth, death, marriage, or property records maintained by state or local government agencies can have actionable consequences for individuals and organizations.

Legal actions related to an organization's failure to protect recorded information may have occurred but gone unreported because they were settled out of court. Arguments in favor of liability for failure to protect records are based on the previously discussed concept of standard of care. Arguments that vital records protection plans are not required by law or not pervasive in a given industry are no defense. The Hooper Doctrine, which dates from a 1928 incident in which a company was held liable for the sinking of barges because it did not equip its tugboats with radio receivers, established the principle that an organization can be held liable for failing to take reasonable precautionary measures, even where such measures may be widely ignored by others.[9]

An organization's senior management bears ultimate responsibility for safeguarding mission-critical information assets, but its involvement is typically and properly limited to delegating authority for the creation, implementation, and operation of a systematic vital records program. To formalize a protection program for vital records maintained by a business, government agency, or other organization, senior management should issue a written directive that:

- Acknowledges the value of recorded information as an organizational asset essential to mission-critical operations.

[9] In re Eastern Transportation Co. (The T.J. Hooper), 60 F.2d 737 (2d Cir. 1932).

© 2016 ARMA International. Purchaser of this PDF file is entitled to print one copy for reference. Other reproductions or redistribution is prohibited.

- Emphasizes the importance of protecting vital records as an integral component of the organization's security policies and contingency planning initiatives.
- Establishes a program for systematic, comprehensive, and economical protection of vital records.
- Identifies records management as the business function responsible for implementing the program.
- Solicits the cooperation of personnel in all program units where vital records are maintained.

As with other records management activities discussed in this book, the development and implementation of a successful vital records program depends upon the knowledge and active participation of program unit personnel who are familiar with the nature and use of recorded information in specific work environments. An advisory committee of program unit representatives can provide a formal structure for such participation. Such a committee can support the records management unit in planning, implementing, and operating a program to protect vital records.

Identifying Vital Records

To be considered vital, a record must be essential to a mission-critical activity, its unavailability must have a significant adverse impact on that activity, and its contents must not be fully duplicated in other records from which essential information can be recovered or reconstructed.

Protection of these essential information assets is an indispensable component of emergency preparedness, business continuity, and disaster recovery initiatives.

Vital records are typically identified by surveying individual program units to determine which mission-critical operations they perform and which records, if any, are essential to those operations. Some mission-critical operations are easily identified and widely encountered. All organizations, for example, must pay their employees, withhold payroll taxes for periodic submission to government agencies, account for pensions and other benefits, collect receivables, and maintain office buildings, factories, warehouses, or other facilities that they own or occupy. Other mission-critical operations are associated with particular types of organizations or industries. A municipal government, for example, must maintain public safety, assess and collect taxes, issue building permits, enforce building codes, and process zoning applications. A healthcare facility must provide patient care. A charitable institution or social services agency must process applications for aid, dispense payments, and otherwise assist those in need. A manufacturer must develop, test, make, sell, and support its products. A law or accounting firm must represent its clients. An insurance company must sell policies and process claims. A bank must process deposits, withdrawals, and other transactions; make loans and collect payments; and safeguard and transfer funds.

© 2016 ARMA International. Purchaser of this PDF file is entitled to print one copy for reference. Other reproductions or redistribution is prohibited.