2006

Electronic Records Management Criteria and Information Security

A Shaw
Edith Cowan University

David T. Shaw
Edith Cowan University

DOI: 10.4225/75/57a81791aa0d3
Originally published in the Proceedings of 7th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia, 4th - 5th December, 2006.

Electronic Records Management Criteria and Information Security

A. Shaw and DT Shaw,
School of Computer and Information Science
Edith Cowan University
dshaw@student.ecu.edu.au

Abstract

Records management practices are mandatory in many business and government operations. Records management is a mature discipline with extensive body of knowledge, professional associations and clearly defined Australian and international standards. Records systems encompass the hardware, software and people necessary for operation and include records generated by and for the system. The Australian legal system has clearly defined standards for admissible evidence in the Evidence Act. Relevant records may require substantial preparation for submission and yet be inadmissible in legal proceedings. The records and system may be challenged in both theoretical and practical senses and appropriate practices and associated records are needed. These records may be expensive to acquire, process and store in suitable format and retaining the original data may be necessary. Applying records from a system to problems outside of the initial system requirements and design may expose the system to attack by showing that it fails to meet good practice. Further, validation of the system may demand suitable records from every stage of the system lifecycle including theoretical and operational basis.

Keywords

Records Management, standards, archiving, evidence, security, reliability

INTRODUCTION

Records assist in determining what actions had which consequences such as contracts and associated financial obligations. Even in antiquity, there were methods to verify content, detect amendments and store the records for future use. From clay tables to paper and to the digital age where records are stored in an electronic format. The clay tablets were baked hard to prevent or detect modifications and sealed in a clay envelope to give extra security and to provide a means of identifying the tablet and information on it. Paper records were stored in the archives where the archivist controlled access and integrity. Confidentiality resulted from restricted literacy of the general population to the digital age where access is restricted by access controls and version controls on the system.

Modern records management and archiving practices in Australia are well established ranging from specialised library collections to multi-national business operations. Australian national standards such as 'AS15489 Records Management' describe recommended practices. The Australian Society of Archivists is the professional association for records management practitioners. The Commonwealth and State governments have established archives for management of records, for example, the National Archives of Australia, and the State Library in WA. Additionally, various specialist libraries maintain collections for long-term reference, for example, the Law Library of the Supreme Court of Western Australia have paper copies of court cases dating back to the 19th century.

The legal requirement for mandatory records keeping is becoming more explicit, for example, after high profile corporate problems such as 'Enron', the 'Sarbanes Oxley' act in the USA establishes new or enhanced standards for all U.S. public company boards, management, and public accounting firms. This requires organisations to be more accountable and to maintain records of their business transactions.

In Australia, there are governing legal environments such as the '*The Electronic Transactions Act*' which defines and regulates aspects of Australian law "*by 'removing existing legal impediments that may prevent a person using electronic communications to satisfy obligations of the Commonwealth law'*."(Allen, 2002 p. 3)

Waltz describes three essential information infrastructure security properties as '*availability, integrity and confidentiality*' with respective Information Warfare objectives as '*disruption or denial, corruption and exploitation*'. (Waltz, 1998, pp.22-23) These information security requirements are directly addressed by record management practices.

In summary, there is a reasonable requirement on a person, company or government to be able justify their actions under arbitration. This is based on record keeping that may be used to demonstrate compliance, resolve disputes and allocate costs and responsibility as needed.

Records and Uses

Keeping of records provides documentary evidence for organisational and societal use. Traditionally, collected data becomes information to produce knowledge but relies on varied technical processes to capture, store, process, retrieve, collate and so on, and requires substantial investment in time and knowledge to administer correctly. From hieroglyphics and cuneiform to ASCII and optical character recognition (OCR), the basic information captured must be preserved for future use.

Records are captured as evidence of business activity, however, there is no uniform implementation and each records management system must be tailored for the specific task. (ASA, 2000, p. 74) Indexing and cataloguing will be specific to the data stored and must facilitate efficient search.

These records systems may require substantial storage, specialised indexing and cataloguing to enable information to be efficiently retrieved. Acceptance of electronic records in legal transactions is now much more common and the differences between electronic and traditional records are of interest.

Paper records, correctly prepared and stored may last over one hundred years of regular use. Additionally, the technologies involved are well established and robust. Methods of detecting amendment, error and misconduct exist. Storage, indexing and retrieval of records have established methods detailed in standards and professional practice. (AS15489, 2002)

Electronic records, in many forms, are readily searched and processed by computers. Additional information available under analysis may extend the working life of a database and generate income from information services. However, there is the possibility that new uses of existing records may cross from 'fair' use to inappropriate use. Further, costs are recovered by selling abstracts for commercial uses such as mailing lists. Of concern, is the possibility that the record may be used to support activities such as investigation and prosecution of alleged crime?

The requirements of an electronic record management system (ERMS) can be found in international documents such as American military standard 'Design Criteria Standard For Electronic Records Management Software Applications' (DoD5015.2-STD), Software Development and Documentation (MILSTD-498) the European 'Model Requirements for the Management of Electronic Records'(MoREQ) among others. This is additional to general standards such as AS15489.

However, the records may be used for purposes other than those in the original capture regime. Basing analysis or conclusions on a data set that was gathered for another purpose and modified or tailored to meet new criteria may be unwise. Professional advice may be necessary.

Record validity, when used in context, is based on the record systems provenance where compliance can be consistently demonstrated. However, new analytical tools such as meta-analysis, data mining among others may create additional information of value. These records when used to support research, decision making or legal action may be subject to major analytical and subjective interpretation. Additionally, the whole system may be

subject to testing and assessment to determine its validity and the quality, subjective or not, of the information. Simply put, if the information system is invalid, then any information from it may be challenged.

Records Management

There is a fundamental difference between electronic documents and electronic records. The Australian Standard AS 15489 states that electronic records differ from electronic documents in as much as they provide evidence in pursuance of legal obligations or in the transaction of business (AS15489, Part 1, 3.15, 2002). Consequently, while a document may stand by itself, a record needs a context.

Standards also address matters to be considered while determining requirements prior to implementing the records system. These requirements may complement but not replace the software requirements and design (DoD 5015.2, MOREQ, 2002). The software lifecycle includes '*Requirements analysis and definition, system and software design, implementation and unit testing, integration and system testing*'. (Somerville, 1992, p. 5)

AS15489.2 states that preservation strategies for records, especially electronic records, may be selected on the basis of their ability to maintain the accessibility, integrity and authenticity of the record over time, as well as for their cost effectiveness (AS15489.2, para 4.3.9.2, 2002). Other methods may be used to retain electronic record integrity, as new technologies become available (AS15489.1 para 8.2.3, 2002). Copying produces an 'identical copy' on similar media while conversion changes the format of a document eg into microfilm. (AS15489-2, 4.3.9.2, 2002)

While paper based records differ from digital records, for example, low technology levels, the digital record cannot exist without hardware and software. This dependence requires that the records and the machines are stored correctly, but when the electronic systems are upgraded then the digital records must be migrated to the new system.

Brooks, in 1986 with his paper entitled ' No Silver Bullet' suggests that '*all successful software gets changed' and, further, 'successful software survives beyond the normal life of the machine vehicle for which it is first written'* (Heap, Thomas, Einon, Mason and Mackay, 2000, p. 361). Brooks continues, the desire for new functions come chiefly from users who invent new uses, however, when the hardware is upgraded they may still use the old software and this may introduce information errors.

Alternately, emulation may be used to create an artificial operating environment suitable to run the software to access the records, for example, a 'DOS' window in a Windows 98 environment. Emulation in software testing practices may have problems, '*The greater the difference between the emulated architecture and the hardware platform the emulator runs on, the greater the complexity of the emulator and the slower it will run.*' (Loveland, Miller, Prewitt and Shannon, 2005, p. 262) This complexity may introduce errors into the software and by extension into the data.

The migration or emulation procedures must include comparison between the original and copied information to base a decision on 'acceptable' error rates. Failure to verify the migration or emulation process may introduce errors that cannot be compared with the original. This process may be time consuming when complicated by the difficulties of maintaining the hardware and software.

When migrating records from one records management system (RMS) to another it may be necessary to extract electronic documents, metadata and audit trails separately. The relationship between these data must be maintained during and after migration. (ASA, 2000, p. 101)

Retaining functioning electronic technologies is not cost effective in an organisation or well supported in traditional museum conservation techniques, where the form not function of the artefact may be important. Further, obtaining suitable spare parts, documents, tools and skills to maintain operation may become very difficult.

Records used as evidence in a court of law must show a chain of accountability and custody that must be shown from the origin or creation through to its initial or primary use. There should be no gaps in the information and

the record must be able to be read by the system when required. This may create problems with out-sourcing of IT functions

When considering a disposal schedule for records some suggested 'rules' from the Standard should apply to records created by the organisation. Disposal should include information that is classed as 'normal administrative practice' such as duplicates and drafts which, when destroyed do not destroy any important information or determine the official record. Documents with numerous copies, newsletters or committee meetings minutes etc should only have the official original copy retained.

The Standards ISO15489.2 para 4.3.9.3. states that records in an electronic form may be destroyed by reformatting or rewriting if it can be guaranteed that the reformatting cannot be reversed. It goes on to state that physical destruction of storage media is an appropriate alternative, especially if deletion, reformatting or rewriting are either not applicable or are unsafe methods.

Analysis of the Records Management System (RMS)

Analysis may include viewing the RMS as a physical system and applying engineering principles to the software and hardware used to produce information. The full information system lifecycle may include '*need, conceptual design, preliminary system design, detail design and development, production and/or construction, utilization and support, retirement and disposal*'. (Blanchard, 2004, p. 15) At all stages of the system existence and beyond there are records keeping requirements.

Methods to control complexity such as systems engineering and reliability analysis are used. Blanchard suggests "*Systems engineering principles shall influence the balance between performance, risk, cost, and schedule.*" (Blanchard, 2004, p. 28) Further, Blanchard continues, '*Reliability can be defined as the probability that a system or product will perform in a satisfactory manner for a given period of time when used under specified operating conditions.'* (ibid, p 33) It follows that changes to the definition of 'satisfactory' or to the operating conditions may affect the probability of reliability.

Complex systems may require extensive system analysis and specification documentation, some of which may become records, and they may be used to verify the design and performance of system hardware. There will usually be a 'system integration test' or 'customer acceptance test' based on these documents where the system operation will be demonstrated.

Loveland et al suggest the difficulty of removing all errors from software and that testing is to '*find the defects that matter.*' (Loveland et al, 2005, p6).

Many test requirements are explicitly stated in the contract; however, there are implicit tests that good practice may require. These may be formally stated in the professional body of knowledge or generally understood as correct professional practice (Jackson and Powell, 1982, pp. 10-12). However, should the system fail to meet expectations, one of the avenues available to the system operator is to impute negligence.

Software components include the firmware, software (operating system) on the hardware platform, the implementation (source code etc) and the algorithm (theoretical methods). Of these, the hardware, firmware and software platform may be outside the developer's control, the algorithms specified and only the implementation and test are accessible. Testing is necessary to verify that the design meets the requirements.

For example, the MD5 Hash algorithm (RFC1321, 1992) specification includes test sequences and results to verify any MD5 implementation. Failure to demonstrate this may be unwise; failure to record the test results may be negligent.

However, testing may be truncated or rushed owing to overruns in the requirements, design and implementation phases to meet contractual delivery dates. Additionally, there are operating procedures, maintenance and training documents that may be needed. Staff training is necessary, defined in standards and subject to review. (ISO 15489.2 para 6.4.2)

All these documents created under the contract and relevant corporate documents may be considered 'records' and used to verify system operation and compliance, meet mandatory record keeping practices and ensure the continuous operation of the organisation. For example, if an organisation cannot locate a record which has been requested under subpoena or Freedom on Information processes, it is more than an annoyance to the organisation it could have serious repercussions. (ASA, 2000, p. 61)

Attacks Against an Electronic Records Management System (ERMS).

There are the common software attacks such as hacking, malware and so on which may be intentional and illegal (Pfleeger and Pfleeger among others). Hardware attacks may be unusual. Unintentional attacks include negligence, incompetence, and stupidity/cupidity of the system users, operators and owners. However, some system attacks may be legal and public, such as media reports of errors damaging user/customer confidence or legal proceedings to elucidate contentions.

The published requirements for electronic records make it easier for them to be used in traditionally paper-based transactions and associated processes. In arbitration, evidence in Australia is governed by the Evidence Act of 1995 and addresses the 'legal admissibility of records created and maintained in electronic systems'. (NAA AA23)

Of concern in legal proceedings with electronic records is the admissibility of the records. Records may meet the Evidence Act requirements and yet not be judged admissible by the presiding judge, or admissible but not used. However, the validity of admissible evidence may be disputed. For example, extending the records systems outside the notional design and test characteristics may adversely affect the quality and utility of the records. Consequently, the whole process that produces, maintains, transfers and manipulates the records may be subject to legal inquiry.

Notional Example of a Records System

A notional public video surveillance system uses optical character recognition to determine the motor vehicle registration to identify the liability for parking and road tax purposes. The image is transmitted, processed and stored and the resultant information is used to interrogate the database to determine the registered owner of the vehicle who is notified in writing of liability for appropriate costs or penalties.

In the notional system, the image is processed with optical character recognition (OCR) software to locate and interpret the image region used to produce a text string equivalent to the vehicle registration. The resultant registration number with associated location and time information may be used to invoice for services, check registration currency or locate a stolen vehicle. However, use of the records for purposes outside the system design may leave the system open to challenge.

A legal challenge to the system may target the error rates in the complete system from electronics to paper. This may require substantial investigation to determine whether the design, implementation and testing has produced a reliable system. Additionally, operating records may verify that system performance has not deteriorated in use. Further, it may require that all its components, tangible and intangible, are verified and acceptable.

For example, hardware reliability may be easily determined from standard engineering techniques and compared with the operating data. Software verification may be more difficult owing to the software diversity and complexity. While an algorithm may be mathematically verifiable, the software implementation on a particular hardware platform may pose a problem.

Implemented algorithms such as optical character recognition, compression, and so on, have error rates. Systems have error rates, further, the information system may be subject to malice, incompetence, negligence and other forms of operator error. The testing must be sufficient to meet potential legal requirements and generate records suitable for the purpose.

The question that is asked is 'do hardware and software systems used in gathering data for legal proceedings need to meet the requirements of good records keeping practices?' In general, the answer is yes, even though

the hardware and software may substantially affect the stored data. Records demonstrating that the system has been operated within the designed parameters may support proof of compliance with accepted standards.

Insufficient reliability may be difficult to measure in-service for comparison with test data. The test data may not be representative of normal operation and frustrate a meaningful comparison. Further, the in-service data may be affected by operation, maintenance and other human activities, as well as affected by malware and inappropriate changes to software.

In cases of major failure, the reparations to customers for associated losses may be excessive and damage system and corporate reputation. In the notional system having to refund a large percentage of the revenues in addition to legal costs may make the cost of a major error prohibitive.

In summary, all aspects of the information system, hardware, software, people and information may be attacked and record keeping will provide the basis of any defence.

Attacking the notional system.

Stallings defines attacks against information flow as interception, modification, fabrication and interruption. (Stallings, 1998) These general attacks may be used against all system information, additionally, there are attacks against hardware and software. Perception management targets the opinions and beliefs of the appropriate persons with a view to altering or controlling their decisions.

Of concern in the OCR process is whether the system can distinguish between the registration plate and any additional text nearby. This may include vehicle badges, accessories and messages such as commercial advertising and bumper stickers. While a normal English word may be extracted from an image and rejected as not having the correct registration number format, there are other ways of encoding data that may create problems. For example, personalised plates may have readable English words such as 'ladyboo' and may be mis-identified as 1ADY800 which may be a valid registration number.

Of interest is 'elite' speak (Leet speak), for example '1337' is used to denote 'LEET' or elite and '47' may mean 'at' instead of '@'. Text transliteration is used to minimise interference from text analysis programs designed to filter out particular words from an information stream.

As an example of 'boggling' (Shaw, Shaw and Maj, 2004), the deliberate introduction of errors into a targeted system, the vehicle owner may consider using temporary make-up to disguise the number plate. Using a whiteboard marker of the appropriate colour to modify temporarily characters in the registration number eg 1ADY336 may become 1ABY886.

Additionally, challenging the tax imposition with the claim of being elsewhere at the time may require the system operators produce the original camera image to permit arbitration. As the arbitration process may take months the bandwidth tied up in storage, retrieval and processing may become substantial unless the records are compressed or deleted. Processes such as compression may introduce data errors, which may cause retrieval errors.

While attacks against the hardware and software are well described, attacks against the theoretical components may be considered. For example, the error rates, applicability, implementation etc of an algorithm. The use of scientific theories in legal proceedings has been addressed in the 'Daubert' criteria that effectively describe necessary criteria to adduce a scientific theory. Criteria include: '1) *whether or not it could be tested and "falsified"; 2) whether it had been subject to peer review and publication; 3) its known or potential rate of error; and 4) whether or not it was generally accepted within the scientific community.*' (Harvard, 2006) Schroeder includes '*the existence and maintenance of standards controlling its operation*' (Schroeder, 2005)

Other avenues may include determining the system is unreliable, proving that its reliability is not adequately determined or showing its reliability has been adversely affected. From this point, the evidential weight may be reduced or negated by the lack of proof of reliability that depends on well-designed records systems correctly

implemented and maintained. Ultimately, the attacker needs to show reasonable doubt exists while the defender may have to prepare to defend the whole system.

CONCLUSION

Compliance with standards is the minimum requirement. Additional requirements may be prescribed or imposed by law after the fact. Compliance failure may be due to negligence and incompetence as well as short cuts imposed by cost cutting. Compliance failure may also result from deliberate attack. Record management requirements address information security requirements such as confidentiality, integrity and availability.

Records of system operation are important and include training of staff, operation procedures, policies as well as system logs for errors, maintenance (preventive and corrective)

Records of system requirements, design, implementation and test with associated user manuals, software maintenance documents are part of the system.

The principal problem then becomes one of record management whose costs must be added to the costs of system acquisition and operation. If the design does not include adequate record keeping practices, then adding them afterwards may be costly. However, the cost of non-compliance may be much greater.

REFERENCES:

Allen, M. (2002). *E-business, the law and you - a guide for Australian business* Prentice Hall Australia.

AS15489 (2002) *AS ISO 15489.1 – 2002 Records Management Part 1. General* Standards Australia

Blanchard, B.S., (2004) *Logistics Engineering and Management* Pearson Prentice Hall

DoD5015.2-STD (2002) *Design Criteria Standard for Electronic Records Management Software* US Department of Defence

Harvard (2006) http://cyber.law.harvard.edu/daubert/ch5.htm accessed 25Sep2006

Heap, N., Thomas, R., Einon, G., Mason, R. and Mackay, H. (2000) *Information Technology and Society* Sage Publications

Jackson, R.M., and Powell, J.L. (1982) *Professional Negligence* Sweet and Maxwell

Loveland, Miller, Prewitt and Shannon (2005) *Software Testing Techniques* Charles River Media

MIL-STD-498 (1994) *Software Development and Documentation* US Department of Defence

MoREQ (2001) *Model Requirements for the Management of Electronic Records* Cornwell Management Consultants http://www.cornwell.co.uk/moreq.html

NAA AA23 Archives Advice No 23 *Providing Electronic Records In Evidence* National Archives of Australia

Pfleeger, C.P. and Pfleeger, S.L. (2003) Security in computing 3rd Edition Prentice Hall PTR RFC1321 (1992) *The MD5 message-digest algorithm* Rivest. R.L.

ASA (2000) *Selected Essays in Record Keeping* Editor J.A. Ellis Australian Society of Archivists

Schroeder, A.T. Jnr. (2005) Evidence based instruction and development: the Daubert approach http://conferences.alia.org.au/ebl2005/Schroeder.pdf accessed 25september 2006

Shaw DT, Shaw, A. & Maj SP. (2004) '*Inducing Errors in Concatenated Databases'* Proceedings of the 5th Australian Information Warfare and Security Conference, Fremantle 25-26 November 2004

Somerville, I. (1991) *Software Engineering* 4th Edition Addison-Wesley

Stallings, W. (1998) *Cryptography and Network Security: Principals and Practise.* 1998, Upper Saddle River, NJ: Prentice Hall.

Waltz, E. (1998) *Information Warfare – Principles and Operations* Artech House London ISBN 0-89006-511-X LoC 98-30140

COPYRIGHT