South African Journal
of Information Management
[DoE accredited]

Peer Reviewed Article

Vol.7(1) March 2005

Preservation of electronic documents in the private sector: business imperative and heritage responsibility

P.J. Lor
Department of Information Science
University of Pretoria
Pretoria, South Africa
peter.lor@up.ac.za

M.M.M. Snyman
Department of Information Science
University of Pretoria
Pretoria, South Africa
msnyman@postino.up.ac.za

Contents

Key words: Electronic documents; electronic document management system; knowledge manager; preservation of electronic documents

1 Introduction

In most organizations today it is difficult to find a typewriter that is still functioning. In today's offices and other workplaces, documentation and correspondence are mostly created electronically: word-processing documents, spreadsheets, databases, and the like. Quite frequently letters and memos created by word-processing software are still printed out for physical distribution by messenger or 'snail-mail'. This is a regressive practice but at least when a letter is printed out, not much information is lost. In the case of a spreadsheet, however, a good deal of the imbedded functionality of the document is lost when a printout is made, the more so if the document is a relational database, a GIS database, or the product of other more specialized software. In these cases, a printout is merely an extract from the information available. It is not a paper equivalent but a fossilized representation, because it does not offer the searching and manipulative functionalities of the electronic document. If the electronic document is lost, the functionality is lost too.

For effective decision making it is necessary to have the most relevant and up-to-date information at hand at the time of the actual decision making. However, organizations are overwhelmed by a burgeoning volume of records and are often unable to locate truly vital information. Compounding this problem is the availability of information in a multitude of formats and the exponential growth in the number of products available. Many organizations are also structured in such a way that business units operate independently of one another, yet they rely on similar information resources. There are often significant gaps, inconsistencies and duplications in information resources within organizations. Therefore, controlling the acquisition, storage and access to electronic information resources is becoming increasingly important.

The subject of this article is the long-term preservation of, and access to, electronic documents in the private sector. We consider the enormous increase in electronic documents, their vulnerability, the importance of preserving them for business, legal and heritage purposes, the preservation challenges they pose, and the role of the knowledge manager in ensuring their long-term preservation and access.

top

2 Rise of electronic documents

There has been an enormous increase in the production of electronic documents in the public and private sectors. Electronic mail, in particular, is increasing at an alarming rate. It is taking the place of both internal memos and letters to external correspondents. Documents produced by word processing, spreadsheet, database and other software are increasingly despatched as e-mail attachments. Some findings from research conducted by the Radicati Group are instructive:

> '[A] typical corporate user in 2003 receives an average of 81 email messages per day, and sends 29 emails per day. This adds up to a total of 110 messages sent/received daily, per user, which represents a growth of about 80% over the daily number of messages sent/received per user only a year ago. While part of this growth can be attributed to spam, most of it is not spam-related and instead represents a legitimate increase in the amount of information exchanged via email.
>
> 'The average size of emails with attachments is also rising. With the growing

> acceptance of electronically delivered documents, such as presentation files, music files, video files, .PDF files, .ZIP files, etc., the average email attachment is now approximately 435 KB in size. This trend is further fueled by the occasional 5 to 10 MB attachment, and the growing prevalence of picture and graphics-laced HTML emails.
>
> 'Our research indicates that in 2003, the average corporate email user sends/receives approximately 9.6 MB of email data daily. Over the next three years, this growth is expected to continue at a rapid pace, reaching 46 MB of email data sent/received daily per user, by 2005' (Radicati and Takahashe 2003).

However, the preservation and management of electronic resources are among the most neglected tasks of the modern organization. Without an adequate information management and archival programme, important records may be misplaced; without proper preservation measures, many valuable documents will literally self-destruct; without precautions, an unanticipated disaster can wipe out irreplaceable information (Choo 2002). This necessitates a higher level of evaluation and control to ensure that quality information is stored and available to those who need it.

Vendors of electronic document management systems have discovered a market with huge potential and are enthusiastically trying to wean organizations from reliance on paper archives by offering systems that they claim will reliably archive documentation in electronic form. Such systems offer many benefits, such as savings in terms of paper, filing cabinets, filing clerks, microfilming and floor space. A further benefit is the speed with which documents and correspondence can be organized and retrieved – from multiple points of view too, since the documents are no longer limited to a single linear order. As organizations adopt electronic document management systems, ever-increasing proportions of their documents will be retained only in electronic form.

top

3 Why retain and preserve electronic documents?

The reasons for retaining and preserving electronic documents fall into three main categories:

- Business
- Legal
- Heritage.

3.1 Business reasons

Businesses need to keep records for purposes of strategic planning, the management of operations, human resources and financial management, etc., regardless of whether these documents are paper-based or electronic. There is a worldwide trend for the adoption of legislation that accords electronic documents the same status as paper-based documents, provided they meet certain requirements. If it is important for an organization to maintain certain paper records, it will in most cases be just as important for the organization to keep those records if they are generated or received electronically.

3.2 Legal reasons

There are numerous laws that require records or registers of various kinds to be retained for varying periods and/or to be made available to inspectors, registrars or other officials, or to other parties or members of the public, as the case may be. Disregarding these legal

requirements can lead to criminal prosecution or civil proceedings, depending on the legislation. Here is the major South African legislation of which we are aware, in chronological order of enactment:

Insolvency Act, No. 24 of 1936
Transfer Duty Act, No. 40 of 1949
Income Tax Act, No. 58 of 1962 [Sections 75(1) and (2)]
Customs and Excise Act, No. 91 of 1964
Stamp Duties Act, No. 77 of 1968 [Section 23(6)]
Companies Act, No. 61 of 1973 (see Regulations for the Retention and Preservation of Records (R2592 of 25 November 1983)
Co-operatives Act, No. 91 of 1981
Close Corporations Act, No. 69 of 1984 (see Regulations)
Stock Exchange Control Act, No. 1 of 1985
Value-added Tax Act, No. 89 of 1991
Occupational Health and Safety Act, No. 85 of 1993
Mutual Bank Act, No. 124 of 1993
Compensation for Occupational Injuries and Diseases Act, No. 130 of 1993
Labour Relations Act, No. 66 of 1995
Basic Conditions of Employment Act, No. 75 of 1997
Skills Development Act, No. 97 of 1998
Promotion of Access to Information Act, No. 2 of 2000
Electronic Communications and Transactions Act, No. 25 of 2002

This list is not exhaustive. For example, we have omitted legislation relating specifically to the public sector, such as legislation on the national archives and public records. It should be borne in mind that most of these acts have been amended at one time or another, in some cases numerous times.

In recent times the *Promotion of Access to Information Act* (PAIA) has attracted much information and comment. PAIA was enacted to give effect to the right of access to information as enshrined in Chapter 2 of the *South African Constitution*. PAIA is specifically concerned with recorded information, regardless of form or medium, and regardless of who created it. As far as records held by 'private bodies' are concerned, Section 50 of the Act states that a requester who demonstrates that a record is needed for the exercise or protection of any right, and who complies with the procedural requirements, must be given access to that record unless there are valid grounds (as set out in Chapter 4) for refusing the request. Private bodies are obliged to compile and make available a manual in which, among other things, they describe the records they hold that are available in terms of any other legislation, as well as the subjects on which the body holds records. This to be done in sufficient detail to facilitate requests (Section 51). A request can be refused if, after all reasonable steps to find it, the record in question cannot be found or if there are reasonable grounds for believing that it does not exist (Section 55). Concealing, destroying, altering or falsifying records with intent to deny a right of access is an offence (Section 90), but being unable to find a record is not. Therefore, unlike some other legislation, PAIA does not impose any specific obligation to preserve records. However, given the existence of a manual describing the kinds of records it holds, a private body would be well advised to ensure that the records listed therein can be found and produced when requested. PAIA has greatly raised awareness of the need to take good care of company records (South Africa 2000).

Originally, the expectation of the legislator was that the records referred to would be paper-based, original documents. Some of the more recent legislation mentioned above allows for records to be produced in microfilm or other reproduced form. However, the landmark legislation in respect of electronic records is the *Electronic Communications and*

Transactions Act, No. 25 of 2002 (Cliffe Dekker Attorneys 2002). This long and complex piece of legislation had a difficult passage through Parliament, because a number of provisions were hotly contested, for example provisions in 'Cryptography providers' (Chapter V), 'Protection of Critical Databases' (Chapter IX), and 'Domain name authority and administration' (Chapter X). The provisions that are relevant to the subject of this article are mainly found in Chapter III, 'Facilitating electronic transactions'. These provisions must be read together with the large number of definitions found in Chapter I.

Part 1 of Chapter III (sections 11 to 20) of the Act deals with legal requirements for data messages. The following are the main points:

- Section 11(1) states that 'information is not without legal force and effect merely on the grounds that it is wholly or partly in the form of a data message'. 'Data message' is an important term and is defined as 'data generated, sent, received or stored by electronic means'. It includes voice (in automated transactions) and stored records. 'Data' are defined as 'electronic representations of information in any form'. The term 'data message' thus covers what we have called 'electronic documents'. Subsection (1) read together with subsection (3) implies that an e-mail message or a letter sent as an e-mail attachment is accorded the same legal status as its paper-based equivalent.
- Section 12 states that 'a requirement in law that a document or information must be in writing is met if the document is (a) in the form of a data message; and (b) accessible in a manner usable for subsequent reference'.
- Section 13 makes provision for a data message to be signed using an 'advanced electronic signature'. An advanced electronic signature is one that has been authenticated by an accredited product or system.
- Section 14 states that information that is required to be presented or retained in its original form can legally be submitted electronically, provided certain conditions are met.
- Section 15 deals with the admission and evidential weight of data messages in legal proceedings.
- Section 16(1) deals with the retention of information in electronic form. This section is cited in full, because it is very relevant to our topic:
  '16(1) Where a law requires information to be retained, that requirement is met by retaining such information in the form of a data message, if–
    a. the information contained in the data message is accessible so as to be usable for future reference;
    b. the data message is in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received;
    c. the origin and destination of the data message and the date and time it was sent or received can be determined.'
- Section 17 states that, subject to certain provisos, 'where a law requires a person to produce a document or information, that requirement is met if the person produces, by means of a data message, an electronic form of that document or information…'

These provisions should be interpreted with care and will no doubt be tested in the courts, but for our purposes they mean that generally, and subject to various provisos which are mainly concerned with ensuring that the documents are what they purport to be, electronic documents have the same legal force as paper documents. This implies that they should receive care of the same standard as is afforded their paper equivalents. It also implies that knowledge managers can expect to have to take care of many more electronic documents.

3.3 Heritage reasons

In addition to business and legal reasons for the preservation of electronic records, there are also heritage considerations. Although there may be only limited legal requirements for their long-term retention and preservation, corporate records have frequently been found to be of great value for historical, social and cultural research. A recent example of research which made good use of company archives is the acclaimed book *In the Company of Diamonds: De Beers, Kleinzee, and Control of a Town*, by Peter Carstens (2001). Carstens made use of De Beers Company Archives and was also given restricted access to Anglo American company records. On a much larger scale, UNESCO has initiated the Slave Route Project. This is a project that forms part of UNESCO's Memory of the World Programme. It comprises wide-ranging research on the Atlantic slave trade and will rely heavily on archival materials such as those found in the archives of companies engaged in the slave trade. Also as part of the Memory of the World Programme, UNESCO is supporting a project to make the archives of the Dutch East India Company (VOC) more widely available. In its heyday the VOC was the largest commercial enterprise in the world. Its archives are a unique source of information on the history of countries throughout the world, including South Africa, Mauritius, Madagascar, India, Indonesia and Australia (UNESCO 2004).

Not every company has as massive an influence on the history of the country in which it is located. But company archives are also a useful source of promotional material and of information for the celebration of company anniversaries.

It is not only archival materials, i.e. *unpublished* corporate records, that are of value to future historians. The long-term preservation of material published electronically by private sector bodies should not be overlooked. Such published records include electronic journals, online databases (such as geographic, bibliographic, and directory databases), and Web sites. However ephemeral they may be and however transient their informational value, these materials are also of value for researchers. Historians researching 19 th century South African history can find a wealth of information in the annual Cape almanacs. Towards the end of the 19 th century these made way for printed directories (Botha 2004). A century later these in turn were increasingly replaced by online databases. If these electronic materials are not preserved, future historians will find the 20 th century much more difficult to research than the 19 th.

Worldwide, national legal deposit legislation is being extended to cover such materials. In South Africa, the *Legal Deposit Act* provides for the legal deposit of electronic publications, including Web sites. Currently a research and development project, funded by the A.W. Mellon Foundation, is under way at the National Library of South Africa to prepare for the implementation of this provision (Lor, Watermeyer and Britz, 2004). However, companies should also accept responsibility for preserving their own electronic publications.

Collecting electronic publications, difficult as it may be to do so comprehensively, is merely the first step in a series of complex curatorial activities for organizing, storing and providing access to the deposited material. We now turn to the preservation challenges that have to be addressed.

top

4 Electronic documents are vulnerable

Electronic document management salespersons hold up to their clients a utopian vision of having all their data comprehensively stored electronically for instant retrieval from their desktops. But things can go wrong, especially in the longer term. There are two main ways in which electronic company data can be lost: through hostile activity or through neglect.

Kasten Chase, a US company specializing in data storage security, warns that a company data centre can be vulnerable to hostile action:

> 'While networked storage provides a number of benefits to data center managers, it also introduces new risks to stored information. Unlike direct-attached storage, networked storage aggregates data, making it an attractive target for external and internal attacks. Data aggregation means that a single breach can have a substantially greater negative impact. Furthermore, removable media such as tapes can be lost, misplaced or stolen. Offsite data mirroring and back-up services often expose valuable data to third parties' (Kasten Chase 2004).

The company points out that e-mail creates particular risks:

> E-mail is a highly flexible tool for business communications and information sharing. In addition to basic messaging, e-mail applications provide file and document storage, contact management features, shared tasks and calendars. E-mail and its attachments often contain proprietary information, or information that is subject to privacy legislation. This information is retained as e-mail files stored on disk or tape. Due to its unstructured format, e-mail data is difficult to monitor, control and classify. As e-mail data grows exponentially and regulations such as Sarbanes-Oxley, require that it be retained, it is emerging as a significant data management challenge. Furthermore, e-mail data stored on back-up media, or entrusted to a third party for off-site storage, creates business risk' (Kasten Chase 2004).

Data are not lost only as a result of hostile activity. Vast quantities of data have been or are being lost in much more benign circumstances. The following are some examples given by a group of librarians from New Jersey, USA, the State Documents Interest Group of the Documents Association of New Jersey:

> 'Though the digital age has barely begun, we have already lost tremendous quantities of data. Digital documents created and stored in legacy software such as COBOL, C/PM, D-Base, WordStar, and even MS-DOS, are now inaccessible to most computer users. The hardware necessary to view information stored on 8” and 5 ¼“ floppies, 8-track and betamax tapes, and other legacy formats has largely disappeared. Government information is not immune from the threat of technological obsolescence. The original raw data from the 1960 decennial census was stored on a then state-of-the-art UNIVAC computer. When the Census Bureau turned the data over to the National Archives in the mid-1970's UNIVAC computers were long obsolete. Heroic and costly rescue efforts recovered most, but not all, of the data. Other items lost to the digital black hole include much of the data from the Viking mission to Mars and pre-1979 Landsat images of the earth. In neighboring New York, all of the computerized data from a comprehensive 1960's study that mapped land use and environmental data throughout the entire state was lost. The study had employed customized computer software that no longer existed when the computer tapes were turned over to the New York State Archives' (Lyons 2001).

Thus, without any hostile intent but through sheer ignorance or negligence, data that cost millions of dollars to assemble, can be lost.

top

5 Why electronic documents are vulnerable

There is a range of factors that can contribute to the unintentional loss of electronic information. We can illustrate this by going back a quarter century in the history of computing, when the names NewBrain, Sord, Lynx, Dragon, Spectravideo, Commodore, Radio Shack and Sinclair Spectrum were well known to microcomputer enthusiasts. These were all makes of mini-computers that proliferated on the market before the IBM PC appeared and became the industry standard. The Sinclair Spectrum came out in the early 1980s with just 1K of memory. A huge range of software was written for it. It is amazing what one can do with one kilobyte. People wrote doctoral dissertations on machines like the NewBrain, which had 32K of memory. Lots of programs were written for all these machines. It was a time of great creativity, when amateurs did much of the programming. This period is part of the history of computing. The games and programs these pioneers wrote remain of historical interest and from that point of view deserve to be preserved. But how much of that period can still be recovered? The tape cassettes that were used for storage are probably unreadable now. The disk formats used by the early Apple are now unreadable to all but a few specialists and, for that matter, so are or soon will be the 360K floppy disks used by the early IBM PCs. The little microcomputers themselves, with their fanciful names, are long obsolete and have disappeared. The machine code in which a lot of the programs were written is unreadable without the machines.

This little excursion into computing history illustrates why electronic documents are vulnerable. The first and most obvious reason for this is the deterioration of the physical media on which programs and data are stored:

> 'All digital documents are stored as computer files on magnetic or magneto-optical media such as computer disks or tapes. Computer files may be erased by accidental exposure to a magnetic field or a surge in electric current. Exposure to oxidation and humidity can cause the substrate material of the disk to degrade. Even with proper storage, digital media degrade over time. According to National Archives, a CD will last from five to fifty years, depending on the quality of its manufacture. The lifespan of magnetic tape, under the best of conditions, is measured in decades. Unless the data is periodically “refreshed” by copying it from one disk to another, it will become unreadable. And when digital data fails, it fails completely. In contrast, archival quality paper and microform can last up to 500 years' (Lyons 2001).

As mentioned in this quotation, this problem can be dealt with by periodically *refreshing* the data, that is, copying it onto a new disk or tape. This is easier said than done, especially if there are large volumes of data to be preserved. A schedule has to be drawn up and rigorously followed to ensure that no data collection is overlooked. The procedures have to be well managed, and this activity must have the full support of senior managers. The problem is that the deterioration of electro-magnetic and optical data carriers is largely invisible. This is in contrast with paper-based documents. Old newspapers and books become yellow and brittle and there are other obvious signs of deterioration such as foxing and mould. Without dramatic evidence of deterioration it may not be easy to persuade the organization to invest resources in the preservation of electronic data.

A second reason is obsolescence of the physical media: new tape and disk formats replace older ones. First there is a period during which both old and new media exist side-by-side, for example 360K 'floppy disks' and 1,44 Mb 'stiffies'. During this period one has to *transcribe* data from the old media to the new media. When data are transcribed from one storage medium to another, by and large there is no loss of data or functionality. The danger lies in postponing this task. It is easy to wait too long. Suddenly one is no longer able to find PCs with both 360K and 1,44 Mb disk drives. How long will 1,44 Mb diskettes still be in use? Many files are now too large to back-up or transport on 1,44 Mb diskettes, so CD-

ROMs or data sticks are used instead. One of these days we will discover that all the data we have backed up on 'stiffies' can no longer be read, because there are no more 1,44 Mb diskette drives.

A third, less obvious, reason for the vulnerability of electronic documents, and one that is potentially a greater threat, is the obsolescence of applications software. Many people who started using PCs for word-processing two decades ago used WordStar, which was then the industry leader. Today, even if the text files are perfectly preserved on a modern storage medium, it is becoming more and more difficult to read WordStar files. They have to be converted to ASCII first and from ASCII to MSWord. It is becoming steadily more inconvenient to convert WordPerfect files to MSWord. Even within MSWord, conversion of text files from older versions to the latest version can become problematic. Typically, the *migration* of programs and data from an older system or platform to a more recent one entails some loss of data, for example font changes and formatting instructions in documents. In database records loss or corruption of data fields may occur.

The final reason for the vulnerability of electronic documents is the obsolescence of hardware and the associated microcode and operating systems. The microcomputers that were mentioned above had their own proprietary operating systems and versions of the Basic programming language, which gave instructions to the CPU and peripherals of those particular machines. A game or software program written for the NewBrain could only run on a NewBrain. The only way to run such programs on a modern PC, if this were necessary, would be to write a program that *emulates* the NewBrain's environment and functionality, that is, create a virtual little NewBrain inside the modern computer. Of course, this requires a good deal of programming. But if we look ten or 20 years ahead, the modern computer in which the NewBrain resides virtually will also be obsolete. So software will have to be written for the PC of 2025 to emulate the PC of 2005. Then the 2025 PC will contain a virtual 2005 PC, which will contain a virtual NewBrain. Later, the 2045 PC will contain a virtual 2025 PC, which will contain a virtual 2005 PC, which will contain a virtual NewBrain... Project this for another half-century and we will have a situation very like the *matryoshka* Russian nesting dolls. There is some disagreement about this among the experts, but it does seem that this cannot be done indefinitely. The alternative is to convert or *port* programs to run on newer operating systems, but this is usually accompanied by some loss of data and functionality. The 'look and feel' is lost. This may not be a big loss if our only interest is in the factual content of the computer files. From the point of view of a scholar studying the history of computing or of computer games in popular culture, it would be a significant loss, however.

The same fate will befall our current laptops and desktop workstations and everything on them – operating systems, software, documents, data files, etc. Electronic documents are subject to what we have ventured to call the 'Law of Predictable Documentary Disaster', which states that the more technologically sophisticated a recording technology is, the more vulnerable documents are to catastrophic destruction. A Babylonian clay tablet, once the cuneiform script has been deciphered, is still legible three or four thousand years later. It is very doubtful whether a 360K floppy disk will be legible 15 or 20 years from now.

top

6 Managing the preservation of electronic documents: the role of the knowledge manager

6.1 Knowledge manager

The knowledge manager is a recent phenomenon created by enterprises to lead and promote

the knowledge management agenda and to help manage a unique organizational asset, namely knowledge (which includes tacit and explicit knowledge). The knowledge manager concept is rooted in the realization that enterprises can no longer expect that the products and services that made them successful in the industrial age will keep them viable in the future (Herschel and Nemati 2000). Knowledge managers have the unenviable task of channeling an enterprise's knowledge into initiatives that are expected to become a source of competitive advantage (Bontis 2002:1). It involves the designing and implementing of a knowledge management strategy and initiatives to support the strategic direction of the enterprise. Apart from the creation of an environment for the sharing of tacit knowledge and the development of an effective information management system, one of the challenges for the knowledge manager is to develop strategies for the effective management of electronic documents. These documents may include:

- Management information, meaning business and administrative data
- Internal documents such as correspondence, notes, minutes, instructions, procedures, e-mail correspondence, etc.
- Published electronic documents such as journal articles, reports, patents, standards, etc. (including internal publications).

The role and responsibilities of the knowledge manager with regard to the management of electronic documents in an enterprise are interpreted differently depending on the needs and environment of the enterprise. However, from the literature (Choo 2002; Earl and Scott 2000; Tiwana 2002; etc.) a number of generic roles and corresponding responsibilities of the knowledge manager with regard to the management of electronic documents were identified.

6.2 Roles and responsibilities of the knowledge manager for the effective management of electronic documents

It is the knowledge manager's responsibility to develop a strategy that dictates how an enterprise handles its electronic documents and to build an electronic document management system to support the business processes. The knowledge manager also has to evaluate the effectiveness of electronic document management projects and their contribution to the mission and objectives of the enterprise. As each organization has unique needs that must be identified and understood, no generic model for developing an electronic document management strategy exists. However, some steps can be envisaged.

The first step in any electronic information management programme is to identify:

- What documents are required to meet the needs of the organization and to optimize the achievement of organizational objectives
- Who needs it
- How it will be used
- Current electronic information sources, services and systems
- How electronic information flows through the organization and between the organization and its external environment
- Current status and shortfalls in electronic document management policies, functions and practices
- Legislation that affects the organization's electronic document management and services (adapted from Henczel 2000; Orna 1999).

To address all these issues, the knowledge manager has to conduct an audit of the electronic documents. Such an audit is a process that will effectively determine the current needs for electronic documents. It establishes what electronic documents are currently supplied and allows a matching of the two to identify gaps, inconsistencies and duplications. The process

also facilitates the mapping of information flows throughout the organization and between the organization and its external environment, to enable the identification of bottlenecks and inefficiencies (Henczel 2000). Various methodologies exist for conducting such an audit (Burk and Horton 1988; Orna 1999; Henczel 2000).

Gaps and deficiencies revealed by the audit should be rectified by the implementation of an electronic document management system for the effective acquisition, organization, storage, archiving and distribution of information, taking into consideration the objectives, corporate culture and organizational structure of the organization.

- *Acquisition*: Planning for electronic document acquisition has become a complex function. Organizations accumulate a huge amount of information about their internal operations and resources. Much of this gathering should be done according to accepted rules, policies, procedures and government regulations. Existing electronic sources also have to be constantly evaluated, new sources have to be assessed and the matching of sources to needs has to be regularly re-examined (Choo 2002).
- *Structure*: To create an organizational memory, electronic information produced and collected needs to be given structure in a way that reflect the interests and information-use modes of the organization and its members, providing access in a manner that is swift, inexpensive and effortless.
- *Preservation*: Electronic document management policies (including records management and archival policies such as records retention schedule) should ensure that significant electronic information concerning the organization's past and present are preserved and made available for use and organizational learning.
- *Packaging*: Electronic information acquired and information from memory should be packaged into different levels of information products and services targeted at the organization's different user groups and information needs.
- *Delivery*: To give end-users the best available information to perform their work, electronic documents should be delivered through channels and modes that 'dovetail well with users' work patterns' (Choo 2002:25).

6.3 Development of an electronic document management system

Electronic document management systems (EDMS) provide organizations with the tools to acquire, structure/organize, preserve and deliver electronic documents. In the planning and development of the EDMS, the knowledge manager acts as designer of directories, systems and protection policies (adapted from Earl 1999:5). The designs are mostly conceptual, in the sense that they work on an idea with a champion, contribute design suggestions and inject thinking from emerging document management practices, as a consultant or system analyst would. The knowledge manager works with and through people, and enlists sponsors, champions and doers and supports clients in inventing, crafting and implementing their own ideas.

For the storage of electronic information and its distribution throughout the organization, technological tools and channels are needed. The choice of technology tools and channels are largely determined by the knowledge manager's understanding of what would work, users perceptions of what they need and the organizational work culture.

For the successful development and implementation of an EDMS, the knowledge manager should take the following prerequisites into consideration:

- Share-ability of documents throughout the organization – more than one user should be able to view a document at the same time
- Capturing of documents received in duplicate in different mediums. Duplicates should

not be allowed
- A single and central repository for all the electronic documents in the organization
- An appropriate registration process to capture registration information (e.g. name of originator, owner, etc.)
- A system which manages documents for their complete life cycle based on the value of the documents to the organization's business
- Strategies for transferring documents to secondary (e.g. magnetic tape) and tertiary storage (e.g. off-site storage)
- Security measures to minimize the risk of loss, corruption and unauthorized access
- Appropriate standards to ensure access is possible across different technological environments, and that documents are accessible over time as technology changes. The document repository should adhere to open standards to allow for seamless integration with other information sources such as existing databases
- A version control plan, which is important to identify the authoritative version of a document
- Enterprise indexing schema, which defines a set of metadata (such as author, title, subject, etc.)
- Provision for free text searching
- The ability to route documents from one user to another in a controlled fashion.

During the design of the EDMS, the knowledge manager should also consider ethical issues such as the following:

- The capturing of knowledge should be based on sound moral principles respecting the autonomy and freedom of people.
- Employees should understand their moral responsibility to 'deliver their knowledge to the repository'.
- Control of access to the document repository must be based on fair principles and not on any form of negative discrimination.
- The quality of information transfer (link to accuracy, reliability) should be ensured (Britz and Snyman 2004).

6.4 Further tasks of the knowledge manager

The management of electronic documents also requires that the knowledge manager should:

- Protect the intellectual property (copyright, patents, trade marks, design rights, customer lists) of the organization by assessing intellectual assets and identifying under-utilized intellectual assets for value extraction
- Oversee adherence to the regulations of the *Copyright Act* (Act 98 of 1978) to prevent the illegal duplication of licensed products
- In accordance to the *Promotion of Access to Information Act* (Act 2 of 2000), ensure that electronic documents are managed in compliance with the instructions of the Act
- In accordance to the *Electronic Communications and Transactions Act* (Act 25 of 2002), ensure that the process of record retention is technically sound and standardized, supported by a policy framework
- Create an awareness and understanding among employees of their responsibilities as electronic record creators and handlers
- Identify immediate training needs in relation to new systems and address the needs
- Identify and appoint committees, teams or individuals for the implementation and maintenance of systems.

top

7 Conclusion

Electronic documents form part of the explicit knowledge resources of any organization. They need to be dealt with in the same planned and systematic manner as the organization's other knowledge resources, whether explicit or tacit. Already electronic resources form the bulk of the recorded knowledge of larger companies, particularly those in the financial and services sectors. If current trends continue, we can expect that this will become the norm in smaller, more traditional companies. We can also expect continued rapid development in information and telecommunications technologies. Twenty years ago e-mail was a primitive, poorly known technology. Twenty years from now the word 'e-mail' may elicit the same blank stares in a freshman information science class as telex and teletext do today. As electronic media proliferate and the volume of electronic resources grows exponentially, they will continue to challenge knowledge managers to devise effective and elegant management solutions.

top

8 References

Bontis, N. 2002. The rising star of the chief knowledge officer. *Ivey Business Journal* (March/April):20-25.

Botha, F. 2004. Nineteenth century Cape almanacs and directories. *Quarterly Bulletin of the National Library of South Africa* 58(2):45-57.

Britz, J.J. and Snyman, M.M.M. 2004. The ethical challenges facing the chief knowledge officer: some critical comments and proposed guidelines. In: *Proceedings of the seventh international conference:Challenges for the citizen of the Information Society, Ethicomp 2004, University of the Aegean, Syros, Greece 14 to 16 April 2004.* Syros: University of the Aegean: 188-200.

Burk, C.F. and Horton, F.W. 1988. *Infomap: a complete guide to discovering corporate information resources*. Englewood Cliffs, NJ: Prentice Hall.

Carstens, P. 2001. *In the company of diamonds: De Beers, Kleinzee, and control of a town.* Athens: Ohio University Press.

Choo, C.W. 2002. *Information management for the intelligent organization: the art of scanning the environment*. 3 rd ed. Medford, NJ: Information Today.

Cliffe Dekker Attorneys. 2002. *Commentary on the Electronic Communications and Transactions Act, 2002.* [Online]. Available WWW: http://www.cliffedekker.co.za/literature/commentary/ect2002.htm (Accessed 24 September 2004).

Earl, M.J. 1999. What is a chief knowledge officer? [Online]. Available WWW: http://lamb.cba.hawaii.edu:82/OldVersions/What%20is%20Chief%20Knowledge%20Officer.htm (Accessed 24 June 2002).

Earl, M.J. and Scott, I.A. 2000. What do we know about CKOs. In: *Knowledge horizons: the present and the future of knowledge management.* Boston: Butterworth-Heinemann: 195-203.

Henczel, S. 2000. The information audit as a first step towards effective knowledge

management: an opportunity for the special librarian. *Inspel* 34(3/4):210-226.

Herschel, R.T. and Nemati, H.R. 2000. *Chief knowledge officer: critical success factors for knowledge management.* [Online]. Available WWW: http://www.brint.com/members/online/20090319/CKO (Accessed 15 March 2002).

Kasten Chase. 2004. *Why data storage security?* [Online]. Available WWW:

http://www.kastenchase.com/index.aspx?id=10 (Accessed 23 September 2004).

Lor, P.J., Watermeyer, H.C. and Britz, J.J. 2004. Everything, for ever? The preservation of South African Websites for future research and scholarship. (Unpublished paper presented at the 6th Annual Conference on World-Wide Web Applications (WWW2004), Johannesburg, 1-3 September 2004).

Lyons, S. 2001. Staying digital: recommendations on preserving New Jersey government information in the digital age; report of the State Documents Interest Group of the Documents Association of New Jersey. [Online]. Available WWW: http://andromeda.rutgers.edu/~govdocs/stayingdigital.pdf (Accessed 23 September 2004).

Orna, E. 1999. *Practical information policies*. 2 nd ed. Aldershot: Gower.

Radicati, S. and Takahashe, T.K. 2003. Email volume and storage growth forecasts. *Messaging Technology Report* 12(9). [Online]. Available WWW: http://www.radicati.com/cgi-local/brochure.pl?pub_id=357&subscr=&back_link=/products/technology.shtml (Accessed 23 September 2004).

South Africa. 2000. *Promotion of Access to Information Act*, Act No. 2. Pretoria: Government Printer.

Tiwana, A. 2000. *The knowledge management toolkit: practical techniques for building a knowledge management system*. Upper Saddle River, NJ: Prentice Hall.

UNESCO. 2004. Memory of the World Programme. [Online]. Available WWW: http://www.unesco.org/webworld/mdm/mow_projects.html (Accessed 24 September 2004).

top

ISSN 1560-683X
Published by InterWord Communications for the Centre for Research in Web-based Applications, Rand Afrikaans University