MANAGING ELECTRONIC MAIL[1]

David Bearman

David Bearman is the editor of *Archives and Museum Informatics.* He served as Director of the National Information Systems Task Force of the Society of American Archivists (SAA) from 1980 to 1982 and is a Fellow of the SAA. He consults internationally on electronic records management for archives, on museum information systems and on descriptive standards. Since 1991 David has made an annual working visit to Australia.

Electronic mail is a new way of transporting communications which creates a new documentary form of record. The question of how to manage electronic mail as a record is one that will confront management in every contemporary organisation within the next few years.

This article explores the issues associated with the management of electronic mail which combine the requirements for correspondence control and filing present in paper-based communications systems with the functional requirements for managing any electronic recordkeeping system. The author applies a generic framework for managing electronic records to define an approach to accountable corporate management of electronic mail. He notes in conclusion that the resultant system provides advantages over traditional paper-based systems in the archives and records management arena as well as for users.

Introduction

In August 1993 the US District Court ruled that the President of the United States, the Directors of agencies within the Executive Office of the Presidency and the Archivist of the United States were wrong in not considering White House electronic mail as records, in not providing for the systematic retention of electronic mail messages, and in believing that they could satisfy recordkeeping requirements for electronic mail by printing certain messages out to paper.[2] The case will not have explicit applicability to other jurisdictions, but the reasoning of the court in a case with such a high profile will certainly not go without notice. The question of how to manage electronic mail as a record is one that will confront management in every contemporary organisation within the next few years. The impetus may be to document what the organisation has done to make better decisions, enforce contracts or avoid claims, or it may be to reduce risks by destroying electronic records as soon as they are not required for operational reasons. In either case we require a framework that will help us ask the question of how to assure that electronic mail results in creation of a record and how to manage records created by electronic mail communications over time.

This paper applies a generic framework for managing electronic records to define an approach to accountable corporate management of electronic mail.[3] The purpose is both to illustrate the applicability of the framework and to assist records managers, auditors and archivists in applying appropriate controls to the creation and maintenance of, and access to, electronic mail. The constants in this framework are:

(1) defined functional requirements for capturing, preserving and providing access to electronic records; and
(2) four tactics used to satisfy any given functional requirement: policy, design, implementation and standards;
(3) rigorous exploitation of the Open Systems Environment (OSE) model of the National Institute of Standards and Technology[4] to identify loci for intervention; and
(4) use of the formal methods of the information science disciplines of data administration and configuration management.

In addition, the framework references the effect of three classes of specific environmental variables:

(1) the business function for which the electronic record is created;
(2) the software in place to support the business application; and
(3) the corporate culture of the organisation.

The methodology is to employ one or more of four tactics to achieve the required degree of control over electronic records throughout their life. The choice of tactics to apply is determined by the variables, based

on an assessment of the ability of each approach, in the specific context, to affect hardware, software or procedure in a fashion that will result in electronic records that satisfy the functional requirements.

To operationalize this method, the functional requirements are viewed as metadata documentation specifications.[5] In this way it is easier to see how they can be satisfied at different points in the overall hardware and software architecture (using the Open Systems Environment model of software architecture) and in the information flow. In consequence, we can express each functional requirement as consisting of a requirement to capture and keep particular metadata at a given layer of OSE or a 'switch' in the hardware configuration and to apply data administration and configuration management techniques to their control.

I. The Problem

We are moving rapidly into a future in which virtually all workers will be linked by networked computing. A decade ago most automation experts predicted that white collar, information workers would lead the way towards this future, but in fact they have held back. Today grocery clerks have networked cash registers, delivery men and messenger services employ networked handheld receipt pads and production workers on the shop floor have networked cutting tools, but many office workers are not yet connected. The economic drivers which have led to value added information processing in the grocery, the factory and the service industry are, however, about to change the office as well. Before this decade is out, information managers will have to support twenty-four hour a day remote access to a virtual work space. Most organisations will provide traditional white collar services, such as advice, regulation and policy debate, electronically. The means by which such communications occur is generically called 'electronic mail', which refers to an underlying utility of software functionality that actually incorporates a changing set of services. Like the Post Office and Federal Express, electronic mail services do not interact with the content of the messages and should support interchange of virtually any kind of data. Indeed, electronic mail can carry highly structured messages such as Electronic Data Interchange (EDI) documents or messages containing data formatted in other than ASCII text, such as multimedia.

Does electronic mail therefore present a problem for accountability and organisational continuity? There is no doubt it will unless organisations do something to manage it. Presidents Reagan and Bush both ordered the erasure of the electronic mail of the White House on the last day of their administrations only to be greeted in court by citizens who successfully argued that the data in these computer systems contained records and could not be destroyed except after

archival review.[6] Electronic Discovery Inc., a Seattle based company, lives by finding electronic mail messages on unmanaged discs throughout corporate America, winning cases and large settlements for its clients in areas ranging from product liability to unlawful personnel practices. As organisations use electronic mail systems in the daily conduct of business, they accrue evidence of the conduct of business that are essential in reconstructing how the organisation made decisions, what decisions it made, and how they were carried out. As some organisations develop and implement policies and procedures, and the auditing, archives, and records management professions define 'best practices' for management of electronic records, organisations will find themselves under great pressure to adopt guidelines and implement programs to control their electronic mail.[7] Even in the absence of such widespread adoption by others, the Appeals Court in the PROFs case admonished the Archivist for dereliction of duty in not providing guidelines and the White House for failing to adopt procedures to assure the preservation of electronic mail.[8]

In our society, organisations are legal persons (i.e. can sue and be sued). They may be committed by their employees when these commitments are communicated in writing or in other ways which leave evidence. Electronic mail is written communication and will become part of the normal business practice of any institution that uses it. Like all writing, it is 'hearsay' evidence but the rules of evidence, business practice, and case law combine to assure that in any jurisdiction, electronic mail will at least be admissible in legal and administrative proceedings.[9]

Organisations are accountable to society. If private, they must provide a reckoning to governmental taxing, regulating, and reporting bodies; if public, they are accountable to the general public, legislative bodies and the executive. In all cases they are responsible for contractual relations and must provide accounting for performance of such contracts. The burden of proof has always been on the organisation, but the trend in many jurisdictions, as illustrated by the adoption of new Federal Rules of Evidence by the US Congress on 1 December 1993, is to place responsibility for identification of all relevant records on their creators.[10] While good recordkeeping was always a valuable defence in court for a company charged with negligence, it becomes essential in a climate in which all records relevant to any corporate activity must be produced within ninety days.

But even if organisations only needed to assure their own survival, we would need to adopt better practices for management of electronic mail. Operational records are required to manage on a day-to-day basis

when an employee is away from the office as well as to survive disasters such as the World Trade Center bombing.

In fact, electronic mail generates requirements for all the functions within an organisation which are dependent upon recordkeeping including privacy administration, vital records management, administrative security, auditing, access and archives. The reasons for managing electronic mail are no different from those for managing internal and external correspondence carried by other carriers, but the functional requirements are quite different.

II. A Theoretical Framework

A. Functional Requirements

The fundamental reason that the functional requirements for managing electronic records seem so different from those for managing records recorded on paper is that electronic records are software dependent. This fundamental property has numerous implications, for example: electronic records are not visible to the naked eye, they require software and hardware to be accessed and used, and they are composed of information created by the integrated use of a variety of software applications. The most fundamental implication is that not all information systems are recordkeeping systems; indeed, most database systems are designed not to generate records when they are queried and provide information in response to a user request even if the user 'writes' a report from that data.

Software dependence dictates that when the records are created they must be identifiable by a system, their boundaries must be known to that system, they must include within their boundaries the complete set of information from whatever software applications is required to assure that they are evidence of a transaction, and the system must somehow assure that a record exists which is comprehensive in that it documents every business transaction. None of these requirements tends to be explicitly identified when we think of paper records because they are either self evident (identifiable, bounded, complete) or nearly impossible to ensure within the design of paper systems (comprehensive).

Software dependence also has an impact on the functional requirements for maintaining records once they are created. The soundness of records, or their integrity as complete records, must be maintained across software generations which may require representing knowledge of their contents, structure and context in system independent ways. Any uses made of them must be audited, including not only changes such as additions, deletions and modifications, but also retrieval, viewing, filing, indexing, or classifying, because these acts have a significance for business and effect subsequent use. In addition, records must be removable under

appropriate authority and exportable to another system in order to accommodate changes in software and hardware systems.

Finally, it is software dependence which makes satisfying the functional requirements for access to records over time difficult. Changes in hardware and software that take place over time can compromise the availability of records to software that will access them, their usability in the ways in which the original record was usable (executing processes along the same relations as the original record when the original record had functionality within a larger system), and the understandability of their presentation to end users because different software than that under which they were created may make different use of the contextual and structural information they contain. In addition, the system must provide for the redactability of records over time and the maintenance of records of redactions across the history of changing implementations.[11]

Even when systems architects, policy makers, and designers of business procedures are alert to these functional requirements of recordkeeping systems, it is not easy to guarantee their satisfaction. Success may rest in the ability of the archivist and records manager to identify an appropriate tactic for the satisfaction of each requirement.

B. Tactics

Assuming a set of defined functional requirements for electronic recordkeeping systems, there are four basic strategies that could be employed to achieve the desired ends. The first is policy.[12] In effect, you could tell people in your organisation to satisfy the functional requirements. If one requirement is to be able to identify the context in which the record was created and the business transaction of which it is a part, you would instruct people in your organisation that they must document this information either in the content of the record or in a header or pointer to the record before it can be communicated to another person. Of course it is possible that a policy may not be adhered to. If this is a risk in a given business context it would lead us to examine one of the other strategies.

We could elect to satisfy the same functional requirement through design. In this case you would specify the development of software which recognized the context from which the record was created, uniquely identified each business transaction, and 'stamped' this information on the record before it was sent out of the system to another individual or database.

Alternatively we could decide to use an implementation approach to satisfying this functional requirement. At logon each individual could be assigned a context extension. Business transactions would be

meaningfully coded by employees as part of a filing system and would be instructed to identify these codes in a second subject line of all outgoing correspondence. The second subject would be employed for retrieval but not transmitted to the addressee.

Finally, the organisation could establish an internal standard, or work to establish a national or international standard, for electronic mail envelope structures which required the presence of such information in order to carry a message across networks. They could then acquire only systems which conformed to that standard.

Over the past several years I have not encountered any approaches to satisfying requirements that use any approach other than these, although most approaches actually combine elements of these four 'pure' tactics. If an organisation walks through each functional requirement for recordkeeping imagining how each of the tactics might be suited to their situation they generate a menu of options for action on electronic records which can be presented to program managers and data processing personnel who are searching for answers to the question of how best to manage such records. The solutions they choose are likely to be dictated by local organisational variables.

C. Variables

There is no rule which defines what tactics an organisation should employ to satisfy each functional requirement, but it must be understood that each requirement can, in principle, be satisfied by a different tactic. In fact, because the functional requirements can be further analyzed to derive a set of metadata functional specifications, there is no reason why each element of information that must be managed in order to satisfy the functional requirements could not come from, and be controlled by, a different tactic. The choice depends on the business function which the records document, the organisational culture in which they are created, and the technological environment or systems architecture in which they are communicated, maintained and accessed.

First, the degree to which each functional requirement pertains must be assessed based on the need to satisfy it in a given functional area. For example, financial transactions involve different risks from personnel transactions. In manufacturing organisations, the background to design decisions are as important as the background to policy decisions are in public organisations. In housekeeping functions, the fact that an action occurred is typically all that it is required to know, and even this may not need to be known for long.

More concrete relationships between business functions and recordkeeping requirements results from specific regulatory and legal requirements for recordkeeping that pertain only to a specific business

application domain. Hence rules under which the organisation operates may dictate the way in which authenticity must be documented or the procedures that must be in place to assure comprehensiveness of documentation of transactions. Often these external rules or guidelines are not so much statutory or regulatory as they are derived from standards of 'best practices' within an application domain or discipline. Thus patient records in hospitals or research records in R&D laboratories are governed by stringent requirements dictated by the practitioners themselves. Sometimes these statements of best practices will be formal, as in the case of ISO 9000 product documentation standards. But more often they have the status of guidelines to a group of professionals but serve as a standard because more formal standards don't exist. When guidelines for recordkeeping exist in a specific business application domain, it is important to incorporate them into the functional requirements adopted for electronic records management in that business context.

Just as the nature of the business functions will influence the approach taken to fulfilling the functional requirements, so will the technical ease of satisfying the requirement through software or system modification. The design of software applications can help or hinder efforts to satisfy the functional requirements through design, implementation and standards. Within a specific application domain, some software packages will serve better and others worse in achieving the same functional end. In developing a tactic for managing electronic records, however, it is critical to understand that application software boundaries are not business application boundaries. In some cases, as in electronic mail, many business applications may be conducted using the same application software (which is, in effect, a utility to the business application). In other cases, a single business application will employ many pieces of application software. In any event, more software than simply application software will be involved in the satisfaction of any business requirement. Strategies for management of electronic records depend on understanding the opportunity presented by the layering of software (the OSE model) and hardware (in distributed systems architectures). Each layer of the software represents a location at which a functional requirement could be satisfied, and every interface between hardware components is a 'switch' across which a communicated transaction must flow.

Technical aspects of the systems environment may provide reasons to address those functional requirements being satisfied through systems design or implementation at particular layers in the software or hardware architecture. Characteristics of the functional requirement or of the technical architecture could lead us to choose to satisfy one requirement through the user interface layer, another

through modification to the application software, a third at the operating system or API layer, and a fourth at the front end to corporate records storage. In the case study that follows, further exploration of these options will illuminate the power of using systems technical features to implement tactics; the point here is that the same technical characteristics may constrain our choice of tactics as well. In an environment in which the software application functionality is a given and proprietary, we may have to locate new functionality at another layer. In a systems architecture in which there are no corporate storage facilities, the 'corporate' view of the local storage may have to be imposed quite differently than in one in which there is a physical corporate store.

Finally, however important technical environmental constraints are, the corporate culture of the organisation (or of the specific business area upon which the strategy is focussed) tends to be the most important variable in selecting the tactics to use in management of electronic records. Some corporate cultures are simply not amenable to certain tactics while others are so hospitable towards them that there is no need to develop more complex approaches. For example, the privacy act administrators in Sweden, when asked how they preserved the rights of individuals in records collected by the government, explained that they simply identified the original purposes for which the information was collected on each file and that the policy stated that the records could not be used for any other purpose. When I expressed surprise that such a policy would be effective, they related to me the case of a minister in the present government who, wishing to use such information for other purposes, asked the Parliament for such an authority but was turned down. What had surprised me was that anyone with custody over such records would be constrained at all in their use, not whether Parliament might be successfully petitioned to alter a use once it was determined. Policy approaches to satisfying access restrictions on records were, in this case adequate, but in another corporate culture these might be unlikely to succeed, leading to the choice of one of the other tactics to satisfy this requirement.

III. Preconditions for Electronic Mail Management

Four critical success factors in implementing solutions to the accountable management of electronic mail are:

- *The identification of electronic records as the information associated with a business transaction.*

  It is inherent in the concept of a transaction that the information must be communicated to be a record. Further, to be considered a record by an organisation, the communication must cross what that organisation regards as a 'business boundary'. Typically the concept

of a business boundary is identical to the boundary of an individual person, so we would say that a record is any information communicated beyond that person. Sometimes however, because of the corporate culture of the organisation, the boundary could extend beyond one person to include that person's administrative assistant, a work team or even a larger group of people. When this occurs it must be clearly understood as a business rule by the employees and the systems that records are only created when information is communicated beyond the boundaries of this larger aggregate.

- *Corporate assignment of responsibility for accountability to every employee in the organisation.*

  It must be understood that records are corporate property and a resource of value which cannot be destroyed or misplaced without serious consequences to the employee. Of course this policy must be accompanied by a training effort to convey to employees a mental model or conceptual framework of how systems in the organisation actually operate and which is adequate for them to successfully carry out this assigned responsibility.

- *Recognition by records managers, archivists, auditors and others concerned with records creation of the primacy of program requirements.*

  Not only must program requirements be acknowledged, but also records managers and archivists need to communicate that attitude to program managers. Once they have succeeded they can begin to convince program managers that the primary reason for good record creation and recordkeeping practices is that it is an operational requirement.

- *It is necessary to understand certain aspects of this software application called electronic mail in order to develop a satisfactory approach to managing the records it produces.*

  Electronic mail is the generic name given to a software functionality which enables users to write a message and 'send' it to another person who may see it on her/his computer at a later time. As a 'store and forward' technology it makes at least one copy of a record of the communication and links it both to the act of creation/transmission and of receipt/opening. It also maintains links between a mail item and responses to it which utilize the 'respond to' software function and to the path of mail that utilizes the 'forward' or 'distribution list' functions. The electronic mail application also maintains names given to documents, security attached to them, and other attributes assigned by the creators. Some electronic mail facilities support extensive indexing attributes assigned by senders and by recipients.

Each of these four critical success factors needs to be explored further if we are to implement electronic mail as a recordkeeping system.[13]

The identification of what constitutes an electronic record is arguably the most critical task in their management. Whatever definition is employed it must be understood by both people and machines since the satisfaction of the requirements will involve a combination of human and system based judgments. In my work for the United Nations in 1989, the suggested definition of a record was as a 'communicated transaction'. We have found this concept workable for both people and machines. It may be more completely stated as:

> A record is any communication between one person and another, between a person and a store of information available to others, back from the store of information to a person or between two computers programmed to exchange data in the course of business.

The important aspect of this definition is that a record is not a collection of data but the consequence of a business event. Records 'occur', rather than 'are'. Electronic data excluded from this definition of records includes information that remains within the computer/workspace of a single individual or the business functional equivalent of a single individual, inaccessible to others, for private information or editing or information stored in a database, but not communicated in a business transaction to anyone else. When the information is shared with another person or sent to or from a machine accessible to others, the transaction in which it is engaged becomes a record. The virtue of this definition is the ease with which individuals can understand it and the simplicity of instructing computing and communications systems to capture it. As we will see in applying the definition in the case study however, it does force people to adopt a more rigorous understanding of what constitutes a record than they have, in many organisations, to date.[14]

The identification of when a record occurs is only the first step, however, in determining what information becomes part of a record. Obviously the content of what is written in an electronic mail message will be part of what is kept, but electronic mail, because of the velocity of communication in this environment, is notorious for assuming that the recipient knows what the message is about. Electronic mail that says 'sure' or 'yes' or 'well done' (to quote a rather famous message from Admiral Poindexter to his aide Bob Pearson upon learning that Oliver North had succeeded in lying to Congress) is frequent. These messages are complete in their content but they lack two other necessary ingredients to make them evidence: structure and context. The contextual data about the message, which tells us who wrote it, when and where it was posted, to whom and with what instructions, is

declared to the software system carrying the message and carried in an 'envelope' when the message is posted outside the originating system. The structure is embodied in the relationships, internal to the message and external, that link the data. For example, the links with prior messages that constitute a train of communications comprising a single business transaction, or the links between text in one file and images in another when both were joined in a single compound document. Content, structure and context must be joined for a record to be evidence.

While the identification of a record is a precondition for managing it appropriately, it will not result in satisfaction of the functional requirements unless the organisation demands, and individuals accept, responsibility for accountability. Unlike paper records which would remain essentially as they were created and interpretable over time even if individuals and their managers did not do anything proactive on their behalf, electronic records are not visible except under software control and are subject to accidental destruction or loss of structural and contextual information if no one takes responsibility for them. Developing policies and promoting consciousness of the need for management of electronic records is only the first step in promoting better practices; it may be necessary to introduce oversight and rewards for information resources management similar to those employed for management of financial, personnel or property resources.

One of the major impediments to employees taking appropriate care of electronic records is that they have a 'mental model' of the way the system works which does not accurately correspond to the way it works in reality. It is no use to insist that employees create or delete records if they do not understand the actual ways in which the systems on which they are working create and delete records. Thus employees may believe that a record which exists on another machine and to which they are pointing is actually in their computer's hard disk or that a record which they have 'deleted' from their system is actually gone when neither is in fact true. Organisations which want their employees to behave responsibly with respect to electronic records must teach them how their system really works so that their mental models will correspond to practice.

Furthermore, no program of records management will succeed unless it is completely clear to everyone involved that the major business of the organisation is the achievement of its mission and that the responsible management of electronic mail is an adjunct function that should in no way interfere with, and may in some ways contribute to, the achievement of the central programmatic missions of the organisation. Electronic mail functional requirements cannot result in the loss of functionality required to perform central missions, produce

necessary products, deliver essential services or develop critical policies. At the same time, recordkeeping requirements are derived from the needs of organisations for continuity of operations and accountability; they are not something external to the organisation and must be weighed in considering the overall costs and benefits of adopting new methods of work and new information flows.

Finally, although the requirements for electronic mail systems are no different from those of traditional correspondence control systems, the fact that electronic mail produces virtual documents (documents whose logical boundaries are not those of a given physical file) does require us to develop some rigorous intellectual constructs to understand these traditional requirements.

To begin with, we need to understand that a record consists of information derived from its content (what the creator writes), structure (relationships between data items maintained by the computer for display and linkage), and context (information documenting the provenance and use of the record).

In terms of content, we need to define electronic mail records as 'what is received'. The content of electronic communications may be edited until they are received by the addressee, but subsequently they must be preserved inviolably.

With respect to structure, mail looks like and acts like what the recipient gets. The record is both what the recipient sees and the software instructions which produce the record in that form from the raw data which is sent. Electronic structural links are analogous to page layout and they may consist of nothing more than formatting instructions, which, while software dependent, do not result in data management problems for which there are not reasonably straightforward solutions. However two other types of structural requirements have been identified which are considerably more challenging to manage over time.

Functionality to link items of correspondence with replies, forwarded materials, enclosures, and any other capabilities supported by the particular application package, must be preserved to form meaningful business transactions. The full web of relationships between records within a business process was once reflected in the collation of all the records having to do with that process in a 'project' file or 'cover' but the interpretation of the actual relationships was left to human beings processing visual and textual clues. In electronic systems these relationships must be managed in part because the business conventions for referencing such relationships are as yet under-developed and in part because they will, in any event, be software dependent.

Functionality to reconstruct active relationships within the data

must be retained whether these are supported by the electronic mail software (which is still very rare) or by the underlying Application Platform Interface (API) layer (which, because of object-oriented toolsets is becoming quite common). The problem can be illustrated by what is often called a 'dynamic document', or a document which embodies active content. In this kind of document, the recipient might see a graph drawn from a spreadsheet created from a database search without necessarily being aware that the graph is not an output product with fixed content, but instead is stored in the electronic mail message as a search query to a database which exports its result to a spreadsheet with embedded instructions. Structural data such as the user permissions set and other limitations on the view of the search database, as well as the database state itself, all go into determining the content of the record.

In relation to context, electronic mail is meaningful, and acted on, because of its source. The context of communications must be preserved with them but it cannot simply be the context which is asserted by the sender (for instance, the date or the distribution). Much attention has been paid to validating of signatures in or to assure correct attribution of authorship, but the more significant aspect of authorization is whether the individual who signed has the authority to conduct the underlying transaction. Electronic correspondence must be authenticated in part because the contents of some electronic mail messages can be designed to take direct effect in the receiving system without being previously assessed by humans.

Further, electronic mail is a store and forward technology. A communication is written by a user at one workstation which has the ability to communicate outside itself and is sent to another user at a different workstation, often through many intervening computers. In the simplest manifestation a user at one workstation attached directly to one computer leaves a message (creates a pointer) for another user at a workstation attached to that same computer. Even here, both users employ all software layers and hardware connections on the way to utilizing the mail although the original message is stored on the same computer which grants access permission rather than having to forward the message. This aspect of electronic mail provides us with significant advantages over paper systems because the entire process exists under the control of a computing technology capable of tracking the mail at every step. In fact, the 'electronic' aspect of electronic mail actually is a great advantage in its management because it provides numerous opportunities for solutions which are not present in manual systems.

IV. Design and Implementation Based Tactics

The problem with managing electronic mail, like that of mail received

through the postal system or inter-office mail, is that electronic mail is a utility. As such it carries undifferentiated types of records for which we have very different business requirements. Since our reasons for keeping records have to do with business requirements for records for ongoing activity or longterm accountability, the fact that we don't know what electronic mail contains, or more accurately what business transaction is carries out, means we don't know how it needs to be managed. We cannot make any progress in managing electronic mail unless we can identify to the system the business transaction it is part of; ideally we would signal this information on an 'envelope' so that the system could avoid having to 'open' the mail and read it in order to make the decision about its management.

One approach that has been taken to identifying the business application source of electronic mail is similar to that used in paper-based systems in which employees categorize their correspondence by assigning it a classification. While the specific method might vary, the implementation is to bring up a screen that the user must fill in before the mailing can go forward. The effect of this kind of approach is that the designation of appropriate management and retention practices is the responsibility of the records creator who is fully conscious that this is what is being requested.

A slightly different approach is to design the user interface so that users do not see 'electronic mail' as an option, but rather view their systems options as business tasks such as 'report on sales', 'send policy directives', 'assign work' or 'make appointments'. The choice of a business task brings up the electronic mail system with appropriate software functionality, pre-designed distribution lists, and style sheets for that task. It also schedules the electronic mail transaction and determines its appropriate storage. Under this scenario the end user is responsible for the effect of sentencing but doesn't consciously make the decision.

A similar approach using the application software layer rather than the user interface is to develop style sheets for different genres of business transactions which carry their sentencing requirements with them. When the user selects an appropriate style sheet, reformatted aspects of the message structure are brought onto the screen and the hidden sentencing information is conveyed along with the transmission.

Combining these approaches, the best solution would be to have users, instead of using software applications directly, open facilities in their user interface for their business purposes such as sending directives, making personal dates, or scheduling staff work. Each user would have an interface designed to support the specific functions of their job. By opening a business application rather than a software application, the use would be declaring in effect what the import of the

message was and how it should be managed. The reasons the user would select the appropriate facility for the proper purpose are both the push of policy and the pull the software capabilities each has already attached. When writing a directive, the style sheet for directives comes up, the distribution list for directives is immediately invoked, and the requirements to acknowledge result in the receipt of each directive being audited. Directives properly distributed through the directives distribution function are tickled for review prior to their expiration date and can be cited as authority in other actions (e.g. are linked to validation tables used elsewhere). Directives cannot be copied locally but are saved only in central records storage where they are available for all to see and so that out-of-date copies are never found in offices. Personal notes, on the other hand, may be secured for viewing by only one person and will be deleted from local spaces after user specified times, but they cannot be saved to corporate storage and may not use corporate styles. Staff schedules use a corporate style sheet, are incorporated into group calendars and individual calendars, and may be answered formally by using calendaring acceptance functions.

Each type of communication employs a variety of other software with preset configurations and thereby facilitates work flow. It also declares the contents of messages for purposes of retention without requiring records managers or archivists to read the contents of each message. Occasional audits can be used to assure that employees are correctly using the functions provided, with training and ultimately reprimand directed towards those not employing the facilities in line with policy.

In addition to being identifiable by the business process for which they were created and in which they served as a transaction, electronic mail must satisfy the functional requirements applicable to all electronic records creation of being comprehensive, complete and authentic.

To be able to prove that the records in the system are comprehensive, the inventory of records in storage must conform to the log of records communicated. Any such log would have to be created by layers of software system below the application, whether the Application Program Interface, the Operating System, the External Environment Interface (EEI) or software at the external communication switches. The inventory would have to be created either as records were read onto a remote records storage device or as a report from the corporate file management software.

To assure that records are complete, a metadata model of the contents of a complete business transaction of the sort conducted under each process would be compared against the contents and envelope of the electronic mail message, perhaps using SGML markup,

to ensure that all the necessary structural and contextual links for that type of transaction were present. A content data model of a complete transaction would, for example, require data for the sender, the recipient, the distribution list, the time of transmission, the time of opening, the response to link (i.e. the context data which says that this message is a response to another user's specified previous message), the response from link (i.e. the data which says that this message is a response from another specified user to a previous message) and any forwarding links.

Authentic transactions are those which originate with the author who claims to have originated and which have authors with the authority to launch transactions of that sort. Both these characteristics of the record can be validated using the information collected to assure completeness or that to assure comprehensiveness. The satisfaction of these requirements could be enforced at the level of the API, where most requirements reflecting security and requiring definite identification of users are resolved, or at the level of the operating system where data is routed to appropriate files. (See Figure 1.)

'Software engines' at communication nodes can stamp electronic mail as it crosses boundaries defined by the organisation as significant for record purposes with respect to specific business processes thus defining 'record transactions' in a way consistent with the UN ACCIS report. Similarly locating such engines at servers, at telecommunication gateways, and in DBMS information retrieval facilities could capture specified types of transactions for forwarding to corporate records stores where they would be documented complete

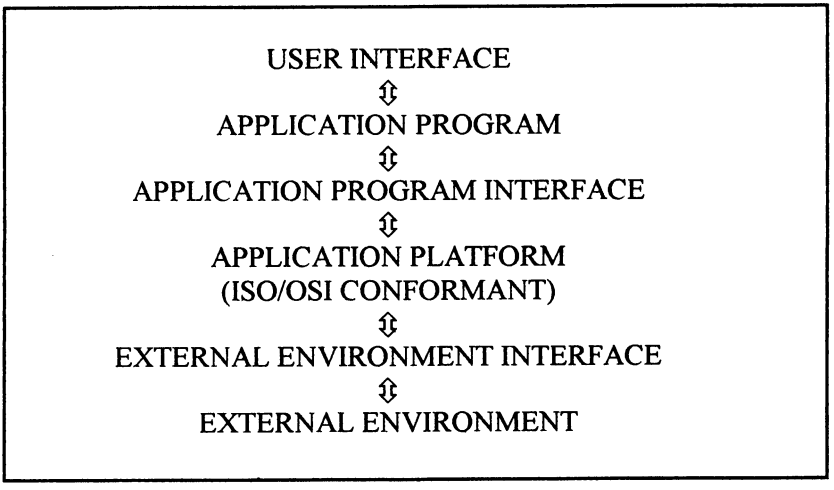

Figure 1. Layers in the Open Systems Environment Model

with the content, structure and context of the transaction and the configuration management data required to reconstruct the information a user would have seen and what functions they would have had available to them. (See Figure 2.)

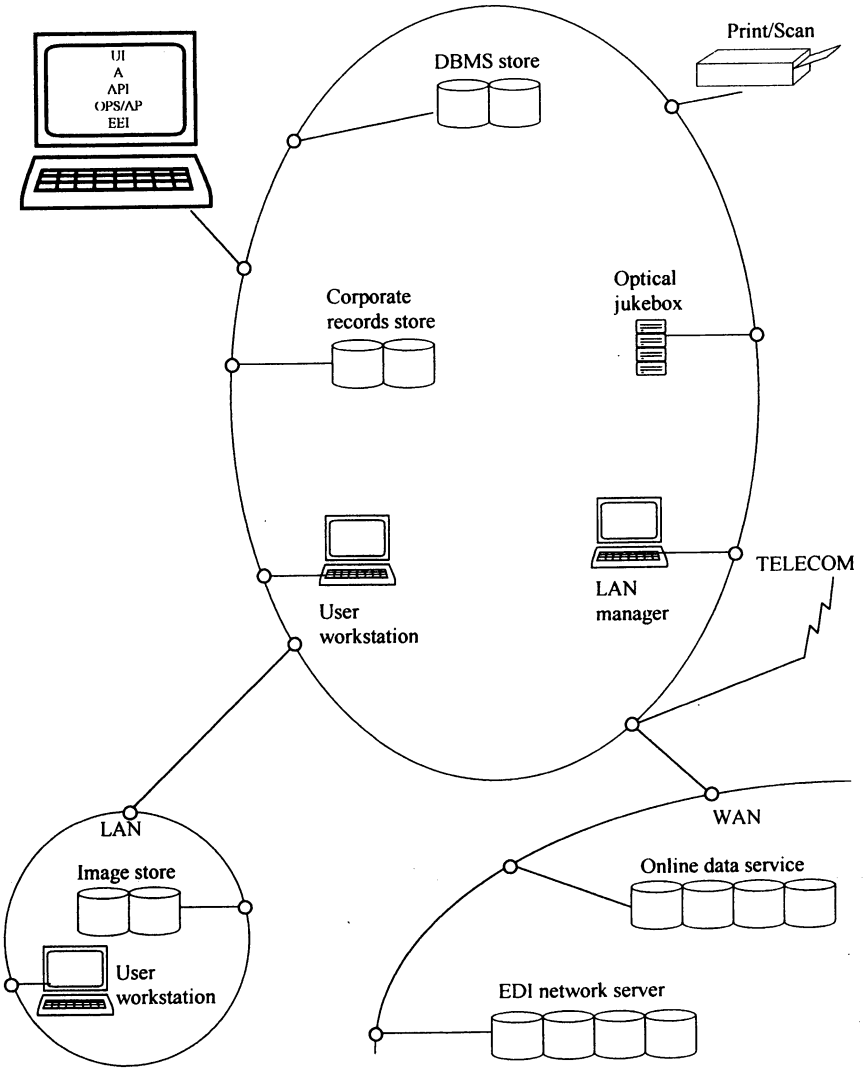

Figure 2. Technical Environment Model

When each functional requirement is reduced to a specification for particular metadata, the system designers and systems administrators can select which 'openings' provided by software and hardware architecture to employ in a specific mechanization of its audit. In principle, each functional requirement could be satisfied by solutions found at nearly every layer of software and hardware and the selection of an actual location at which to intervene should reflect the requirements of the specific organisation and its actual architecture.

It will often be easier to obtain the same result at one layer or another because of the tools available in an organisation or the assignment of responsibility for control of different portions of a system to different agents within the organisation. If the tools for user interface design are not flexible enough to support the proposed solution of structuring the interface to reflect the business transactions of the organisation (and hooking the appropriate software functionality to those functions), we could turn to another layer. For example, the approach of building software to monitor communications traffic from the user workstation as it enters the network (becoming available as corporate records) might prove viable. Also it may be necessary to use solutions at communication interfaces if the network administration control is tight but the local workstation use control is weak; or it may be desirable to build the functionality into corporate record stores and ignore local filing and storage facilities if there is little corporate ability to influence naming conventions used by those with control over local workstations.

Implementing responsible solutions to electronic records management can be made easier in the future by adopting architectures that take advantage of some relatively new approaches to computing. Object oriented systems, when they are implemented, will allow us to attach object attributes to records that cause them to be filed, retained, and accessible in the ways that a records policy would dictate. Client-server architectures allow us to build servers that will continue to perform their role across generations of clients and clients that can address new servers when these are needed making for easier and less costly migrations. Open systems standards if adopted will generally make the task of managing distributed information resources over considerable periods of time much easier and may lead to areas of interoperability even if complete interoperability eludes us. Existing standards in the electronic mail area have already made internetwork interchange more possible. With appropriate extensions, the X.400/500 standards could accommodate contextual and structural information needed for reconstruction of evidential historicity.[15]

One of the outstanding issues in the management of electronic mail and other electronic records concerns whether to write a

representation of the structural and contextual information to the record or retain it in the external environment. If we write a representation to the record, essentially adding the information as an extension of the content of the record itself, we can take advantage of the software independence of ASCII code to convey structural and contextual information. The disadvantages of this approach, and the advantages of retaining it in its original software environment, are (i) that we have to open the message to identify its author, business application source, date, the web of interlinked messages and other structural and contextual meanings, and (ii) that we will have to use great care in selecting a method of representation that will preserve our ability to manipulate the representation for purposes of automatically reconstructing structural links.

In an ideal world, the envelope defined by the standard interchange protocol X.400 would accommodate this necessary data, but because the need for this metadata relates to post-receipt understandability and usability rather than to transmission, the X.400 protocol, which restricts itself to carrying data essential to successful transmission, does not provide this facility. On the other hand, the contextual and structural data is directly related to the success of the directories defined by X.500 and the archival and auditing professions have a strong position with respect to the viability of such directories over time if they care to make the case to appropriate standards bodies. It should be noted, however, that within our community we do not yet have accepted definitions of the essential contextual (provenancial) metadata nor developed methods of representation that could be commonly employed to indicate the kinds of structural links we feel it essential to represent.

Defining the essential metadata for structural and contextual documentation of electronic communications is one of the tasks being undertaken in a research project at the University of Pittsburgh.[16] One purpose of such metadata would be to permit the management of 'corporate memory'[17], whether in central corporate storage or distributed systems by identifying the attributes that would serve as filing headers such as project titles, names of recipients, dates or accounting codes as well as file classification.

Once designated to the corporate records store, the issues respecting the management of electronic mail become those of managing electronic records in general. The requirements which must be satisfied in their maintenance are that they remain sound, auditable, exportable and removable. These properties are largely assured through standard data centre system security and auditing applied with an understanding of the boundaries of the original electronic record, boundaries which incorporate content, structure and context information.

Similarly, access to electronic mail stored as a corporate record involves the same measures to satisfy requirements that the record be available, usable, understandable and redactable that would be applied to other records. These measures rely on systematic and continuous configuration management practices applied to both software and hardware with an understanding that records can only be made available, usable and understandable over time if they are migrated to current systems. It also recognizes that migration is extremely dangerous both because it risks accidentally changing record linkages and functionalities and because it necessarily takes place in an interstice between two auditable systems.

Conclusions

Electronic mail is a new way of transporting communications which creates a new documentary form of record. The issues associated with its management combine the requirements for correspondence control and filing present in paper-based communications systems with the functional requirements for managing any electronic recordkeeping system. The tactics available for managing electronic mail are those which are generally available for managing electronic information systems. The conceptual framework developed for the management of electronic records of any sort can be applied to electronic mail. When we apply this framework it becomes clear that electronic mail is a utility which can only be managed if the business application which the communication supports is clearly identified up front because the requirements we place on the subsequent management of the record are a product of the appraisal, scheduling and sentencing of records of that business application.

As a new documentary form, electronic mail is not governed by many conventions. In its management we are forced therefore to educate the users about how these systems and our in-house files work, design systems that recognize records of specific business functions and treat them accordingly, implement systems which segregate the creation and storage locations so that records must cross over software switches that can assess how they should be managed, and deploy standards that contribute to better documentation of the content of electronic mail, particularly metadata documentation standards.

When this framework is applied to electronic mail, the resultant system should be more manageable than traditional paper-based systems both from the perspective of executing appropriate dispositions and from the view of users who want to retrieve records in the future.

ENDNOTES

1. Previous versions of this paper were delivered at the Society of Canadian Office Automation Professionals, Ottawa, 31 March 1993 and the National Association of Government Archives and Records Administrators Annual Conference, St Paul, Minnesota, 22 July 1993. Ideas contained in the paper were refined in workshop presentations at Monash University, Melbourne in June 1993 and the University of Texas, Austin in November 1993.
2. 'Federal Appeals Court Rules Against White House in PROFs Case' Special News, *Archives and Museum Informatics*, vol. 7 no. 3 Fall 1993 and 'The Implications of Armstrong v. the Executive Office of the President for the Archival Management of Electronic Records', *American Archivist*, forthcoming, vol. 56, Fall 1993.
3. Other papers by David Bearman explaining this generic framework include: 'Archival Data Management to Achieve Organizational Accountability for Electronic Records', *Archives and Manuscripts*, vol. 21, no. 1, 1993, pp. 14–28; w/Margaret Hedstrom, 'Reinventing Archives for Electronic Records: Alternative Service Delivery Options' in Margaret Hedstrom, editor, 'Program Strategies for Electronic Records', *Archives and Museum Informatics Technical Report* No. 18, 1993, pp. 82–98.
4. Gary Fisher, 'Application Portability Profile: The U.S. Government's Open System Environment Profile', National Institute of Standards and Technology, April 1991, NISTSP 500–187.
5. For a useful overview of the concept of metadata in archival documentation, see David Wallace, 'Metadata and the Archival Management of Electronic Records: A Review', *Archivaria*, no. 36, Autumn 1993, pp. 87–110 and David Bearman, 'Documenting Documentation', *Archivaria*, no. 34, Summer 1992, pp. 33–49.
6. 'Federal Appeals Court Rules Against White House in PROFs Case', 'The Implications of Armstrong v. the Executive Office of the President for the Archival Management of Electronic Records', op. cit.
7. Canadian General Standards Board, 'Microfilm and Electronic Images as Documentary Evidence', CAN/CGSB-72.11-93; also note ISO 9000/9001.
8. In their decision in Armstrong v. the Executive Office of President, the US Federal Appeals Court stated:

   > Under the FRA, the Archivist's duties are not limited to judging the suitability of records for disposal. In addition, the Archivist must 'provide guidance and assistance to federal agencies with respect to ensuring adequate and proper documentation of the policies and transactions of the Federal Government and ensuring proper records disposition'. Id 2904(a)

9. The *Federal Rules of Evidence* and the *Uniform Rules of Evidence* used by most states in the US, as well as the *Federal Business Records Act* and *Uniform Photographic Copies of Business and Public Records as Evidence Act* (UPA) also used by most states in the US, essentially support the use of electronic records if they are employed in the normal course of business, in a manner that is compliant with law and are used in an accountable fashion (responsible, reliable and implemented).
10. The *Federal Rules of Evidence*, as amended 1 December 1993, require records creators to reveal, within ninety days of the filing of a case against them, all records that might be pertinent to the case without having opposing counsel request them under discovery procedures. Freedom of Information and Privacy laws in many countries which are beginning to require governmental bodies to list the records that they create on citizens or the record systems they maintain for FOI queries, are consistent with a trend towards up front declaration as are proposals such as the US Government Information Locator Service (GILS).
11. Redaction refers to the process of covering portions of a text prior to release in fulfillment of a privacy or Freedom of Information request in order to protect privacy or security interests. The redaction does not alter the original so the full text

will be available for subsequent release or on release to someone with different security clearance. The issue for functional requirements is to keep track of different redactions since release of a document is a transaction of importance and the actual version released is a matter of record.

12. This is examined at considerable length in my 1990 report to the United Nations. The report, in a slightly edited form, was published at chapter 2, 'Management of Electronic Records: Issues and Guidelines', in United Nations Advisory Committee for Coordination of Information Systems, *Electronic Records Management Guidelines: A Manual for Policy Development and Implementation.* NY, United Nations, 1990, pp. 17–70, 89–107, 135–189.
13. David Bearman, 'Record-Keeping Systems', *Archivaria*, no. 36, Autumn 1993, pp. 16–36.
14. For a fuller elaboration, see David Roberts, 'Defining Electronic Records, Documents and Data' elsewhere in this issue of *Archives and Manuscripts.*
15. The concept of evidential historicity is developed further in David Bearman, 'Archival Principles and the Electronic Office', Angelika Menne-Haritz, editor, *Information Handling in Offices and Archives*, K.G. Saur, New York, 1993, pp. 177–193.
16. Further information, including a bibliography of publications of the research findings of the project, can be obtained from Richard J. Cox, Assistant Professor, School of Library and Information Science, University of Pittsburgh, Pittsburgh PA 15260 or via Internet from rjc@lis.pitt.edu
17. The term 'corporate memory' is widely used by the Canadian government in its policy frameworks for management of electronic records, in particular by John McDonald of the Information Management Practices and Standards Branch of the National Archives of Canada and by the Treasury Board Secretariat.