Moments of Risk: Identifying Threats to Electronic Records*

DAVID BEARMAN

RÉSUMÉ L'auteur a quitté le domaine des documents électroniques il y a dix ans, puis il y est retourné afin d'examiner ce qui à l'époque semblait être un champ de bataille de positions irréconciliables. Depuis 1997, des points de convergence significatifs semblent être ressortis. Ce texte identifie six « moments de risque » qui se produisent lors de transitions d'états critiques dans la vie des documents : l'enregistrement, le maintien, l'ingestion, l'accès, la disposition et la préservation. Il examine la littérature de la dernière décennie dans le but d'identifier les critères généralement reconnus selon lesquels on peut savoir que les documents ont réussi à traverser ces moments de risque indemnes. En repérant les points critiques dans la vie des documents et les critères selon lesquels nous pouvons nous assurer que nos méthodes de gestion ont réussi, il espère préparer l'arrivée de tests qui pourraient être acceptés par les défenseurs de différentes stratégies.

ABSTRACT The author left the field of electronic records a decade ago, and has returned to survey the landscape of what at that time appeared to be a battleground of irreconcilable positions. Since 1997, significant areas of agreement seem to have emerged. This paper identifies six agreed "moments of risk," which occur at critical state transitions in the life of records: at capture, maintenance, ingestion, access, disposal, and preservation. It examines the literature of the past decade to identify the commonly held criteria by which records can be known to have survived such moments of risk unscathed. By locating widely accepted critical points in the life of records and the criteria by which we can assure ourselves that our management methods have succeeded, it hopes to make way for tests that could be agreed between proponents of different strategies.

Introduction

The author ceased doing active research on archiving electronic records in late 1996, though his publications on the subject continued to appear in the literature until 1997. When he left the field, it seemed that various players had established orthogonal positions, not just on how electronic records should be

* My thanks to Terry Cook, Wendy Duff, and Jennifer Trant who read and edited drafts of this paper, and to the anonymous reviewers for their suggestions.

managed, but even on what they were, on why they were an issue, and on the objectives of electronic records and archives programs. Returning to the field a decade later, a review shows the differences that seemed so irreconcilable then, appear now more like different tactics to achieve strategically similar objectives.

Indeed, by asking what various research traditions view as the most critical moments in the life of records, and identifying the criteria each tradition uses to evaluate its success at overcoming the risks to "record-ness" identified with those moments, we expose a significant amount of agreement both on the basic threats to electronic records and on how to assess tactics for successful records management – from creation through disposition – and archival management, from ingest through preservation and access. There are still a number of divergent proposals about how best to implement electronic record-keeping and electronic archives management, but the central strategic questions may have been quietly resolved. If so, this emergent agreement provides the foundation for a variety of solutions that satisfy a set of widely accepted criteria. The weaknesses in approaches that do not fully satisfy these criteria can be identified, and possibly addressed.

After exploring a framework for strategic agreement, and examining some proposed tactics, this paper looks at efforts currently underway in a range of countries to see how they address the identified challenges.

Electronic Records Projects of the 1990s

Prior to the 1990s, pioneering archivists who paid attention to machine-readable records developed methods to document files transferred to them on magnetic tape from routine computing systems of large agencies, including, importantly, statistical and census data sets. With the advent of widespread office automation and networking however, the everyday records of government and business were increasingly produced and received electronically, calling methods developed for archiving data files into question.[1]

In 1990 the United National Administrative Coordinating Committee on Information Systems made recommendations on policies for Electronic Records Management.[2] Policy documents since then have broadly agreed on

1 For a review of American programs and major thinkers, see Richard Cox, *The First Generation of Electronic Records Archivists in the United States* (New York, 1994); for a critical assessment of how and why the transition occurred in the National Archives of Canada, see Terry Cook and Eldon Frost, "The Electronic Records Archival Programme at the National Archives of Canada: Evolution and Critical Factors of Success," *Archives and Museum Informatics* 6 (1993), pp. 38–47; and Terry Cook, "Easy to Byte, Harder to Chew: The Second Generation of Electronic Records Archivists," *Archivaria* 33 (Winter 1991–92), pp. 202–8.

2 United Nations, Advisory Committee for Coordination of Information Systems (ACCIS), "Electronic Records Management Guidelines: A Manual for Policy Development and Imple-

the issues that needed to be addressed,[3] but the fundamental limitations of policy as a means of controlling electronic records management have been readily apparent since the early 1990s. Ultimately end-user organizations have been unable to implement policies even when they understood the need for them, since they lacked the technical ability to control distributed electronic records effectively and individual users did not have appropriate tools or mental models of the systems to help ensure that controls would function. What was needed was to move beyond solutions dependent on policy alone, to those which implemented systems-based control.

In 1991, the US National Historical Records and Publications Commission convened a Working Meeting on Research Issues in Electronic Records.[4] The resulting report identified ten "open" questions, and focussed attention on the first three:

- What functions and data are required to manage electronic records in accord with archival requirements? Do data requirements and functions vary for different types of automated applications?
- What are the technological, conceptual, and economic implications of capturing and retaining data, descriptive information, and contextual information in electronic form from a variety of applications?
- How can software-dependent data objects be retained for future use?

The NHPRC invited proposals on any of the open questions, and funds were allocated to a number of projects in the following years.[5] The most ambitious of these, the "Pittsburgh Project" ran at the University of Pittsburgh from February 1993 through the summer of 1996,[6] and prepared the way for a number of follow-on studies that tested its propositions.

---

mentation" (New York, 1990). The author, who was the principal author of the draft ACCIS policy recommendations, believed at the time that policy and careful definition of what was meant by records could largely resolve the problems we identified.

3 Public Record Office/e-Government Unit, "E-Government Policy Framework for Electronic Records Management," (London, 2001), available at: http://www.nationalarchives.gov.uk/electronicrecords/pdf/egov_fra mework.pdf (accessed 12 September 2006).

4 The report of this meeting, National Historical Publications and Records Commission, "Research Issues in Electronic Records" (Washington, DC, 1991), was influential not just in setting NHPRC directions (it was unanimously endorsed by the NHPRC at its June 1991 meeting), but in defining what the profession thought to be the open questions.

5 For a list of projects in this area funded by the NHPRC from 1979 through 2002, see: http://www.archives.gov/grants/electronic_records/projects.html (accessed 12 December 2004).

6 Richard Cox, on the faculty of the University of Pittsburgh, served as principal investigator. The author was the lead consultant. Wendy Duff, David Wallace, Kim Barata, and other students played significant roles in the project over the three years. See the project proposal at http://web.archive.org/web/19991217190724/http://www.sis.pitt.edu/~nhprc/IProposal.html (consulted 12 December 2004). It is ironic that the University of Pittsburgh, a higher educa-

In Canada, Luciana Duranti's project on Preservation of the Integrity of Electronic Records at the University of British Columbia reached the conclusion of it theory-building first phase in 1996,[7] and began its evolution into InterPARES, a massive international undertaking involving players from throughout the world. Simultaneously, the International Council on Archives' Committee on Electronic Records was formulating its major guide to electronic recordkeeping.[8]

Conclusions Reached by 1997

However, by 1997 the degree of consensus was overshadowed by competitiveness between the two major North American projects, compounded by fundamental differences in their methodologies that made it hard for them or others to see underlying commonalities or credit each other's useful insights. The Pittsburgh Project prided itself on using a bottom-up approach, that made no assumptions from archival traditions, to derive a totally pragmatic answer to the question of how best to manage records. The UBC Project had equal pride and faith in a top-down approach, informed by archival tradition and theory, and grounded in the way that archives have been managed in the Western world for centuries. These philosophical differences, together with resulting differences in their use of language, exaggerated the gap between their understanding of the problems and proposals for solutions.

Both projects agreed that electronic records were created in the course of conducting business or personal affairs, that documents resulted, and that documents were communicated from a sender to a receiver. Both projects agreed that metadata would need to be attached to, and kept with, records over time, and that this metadata would document the content, structure, and context of the records, an analytical framework that since its introduction in 1992[9] has been universally adopted. This important two-pronged consensus was reinforced in a somewhat wordy definition by the International Council on Archives in 1997:

A record is recorded information produced or received in the initiation, conduct or

tion institution devoted to digital libraries, lost its only copy of the documents from this research project and that copies are now available only on the "Wayback machine" and the websites of individuals associated with the project.

7 Luciana Duranti and Heather MacNeil, "The Protection of the Integrity of Electronic Records: An Overview of the UBC-MAS Research Project," *Archivaria* 42 (Fall 1996), pp. 46–67.

8 ICA Committee on Electronic Records, "Guide for Managing Electronic Records from an Archival Perspective," ICA Studies #8 (Paris, February 1997).

9 David Bearman, "Information Technology Standards and Archives," *Janus* 2 (1992), pp. 161–66.

completion of an institutional or individual activity and that comprises content, context and structure sufficient to provide evidence of that activity …[10]

One difference in tactics was amplified by the ideological divide between the Pittsburgh and UBC projects. As a matter of convenience, the Pittsburgh Project treated everything thus transmitted as a record, though it might have a "retention period" of seconds, because it allowed a single method of capture to be employed for everything; the UBC Project, following a more traditional approach, treated as records only documents that were kept and filed by the agency. The Pittsburgh Project sought means to generate metadata automatically necessary at the capture phase from the business process that gave rise to records, while the UBC Project, because it located responsibility for registering and classifying records with the record-keepers in the agency, envisioned classified records and record series, much like those that once existed for physical records.[11] Both projects believed that archival control was crucial to preserve the authenticity and reliability of records. However, because this author argued that if records were captured up front, and controlled according to archival principles, it did not matter where they were physically housed, to whom responsibility for archival control was assigned, or whether they were ever "transferred" to a dedicated archival agency[12] (a position that seemed heretical to the UBC Project[13]), agreement on the requirement for archival control was seen as a matter of dispute about custody. But despite the emotion this question generated,[14] all the reports surveyed agree that electronic records must be kept under the control of trusted record-keeping authorities and systems at all times.

Records should be made and maintained in a trusted record-keeping system and preserved by a trusted custodian. A trusted record-keeping system comprises the whole of the rules that control the creation, maintenance and use of the records …[15]

10 ICA Committee on Electronic Records, "Guide for Managing Electronic Records," p. 7.

11 Jim Suderman, "Defining Electronic Series: A Study," *Archivaria* 53 (Spring 2002), pp. 31–46.

12 David Bearman, "Archival Strategies," *American Archivist*, vol. 58, no. 4 (Fall 1994), pp. 374–407.

13 Terry Eastwood, "Should Creating Agencies Keep Electronic Records Indefinitely?," *Archives and Manuscripts*, vol. 24, no. 2 (1996), pp. 256–67.

14 David Bearman, "An Indefensible Bastion: Archives as a Repository in the Electronic Age," in David Bearman, ed., *Archival Management of Electronic Records* (Pittsburgh, 1991); Eastwood, "Should Creating Agencies Keep Electronic Records?"; Terry Cook, "Leaving Archival Electronic Records in Institutions: Policy and Monitoring Arrangements for the National Archives of Canada," *Archives and Manuscripts* 9 (1995) pp. 141–49.

15 InterPARES Strategy Task Force, "Strategy Task Force Report," (2001), p. 4, available at: http://www.interpares.org/book/interpares_book_g_part4.pdf (accessed 12 September 2006).

To be evidence, records must be inextricably linked with their metadata and inviolable in their content for as long as they are kept. Where they are, physically, is irrelevant as long as they are properly protected and controlled.[16]

The state of play was summarized in the presentations made to the 1997 Electronic Records Research conference (sponsored by *Archives and Museum Informatics*) attended by representatives of most of the institutions and projects working on electronic records internationally at that time. The documents from that meeting comprised a vast collection of previously unpublished research papers and background reports.[17]

Following the 1997 working meeting, the conveners reported to the broader digital library community on the agreements archivists reached on records as consisting of content, context and structure, as evidence of transactions, and as requiring metadata expressions of business processes.[18] They stressed the urgent need for a concrete semantics and syntax of e-records metadata, for methods of auditing policies designed to ensure accountability, and for methods of recognizing record creating events and determining needs for evidence. In addition, they identified less time-critical but essential research needed on how best to classify the records once "set aside" (characterized as capturing metadata and binding it to records), on registering records (viewed through a lens of encapsulation mechanisms), and of repertoires for format migration.

Elsewhere in the archival literature of 1997, Margaret Hedstrom, the ICA Committee on Electronic Records, Paul Marsden, Barbara Reed, and Heather MacNeil all summarized what they saw as the state of play. Each can now been seen to have over-emphasized the differences between the projects, positions, and approaches.[19]

16 David Bearman, "Item Level Control and Electronic Recordkeeping," *Archives and Museum Informatics*, vol. 10, no. 3 (1996), pp. 195–245, available at: http://www.archimuse.com/papers/nhprc/item-lvl.html (accessed 12 September 2006).

17 These were placed on the World Wide Web for rapid dissemination (http://www.archimuse.com/erecs97/index.htm) and an extensive meeting summary was published in *Archives and Museum Informatics*, vol. 11, nos. 3–4 (1997). The author's summary of some of the issues going into the meeting appeared as David Bearman, "Capturing Records' Metadata: Unresolved Questions and Proposals for Research," *Archives and Museum Informatics*, vol. 11, nos. 3–4 (1997), p. 271.

18 David Bearman and Jennifer Trant, "Electronic Records Research Working Meeting, May 28–30, 1997: A Report from the Archives Community," *D-lib Magazine* 3 (July–August 1997), available at: http://www.dlib.org/dlib/july97/07bearman.html (accessed 12 September 2006).

19 Margaret Hedstrom, "Building Record-Keeping Systems: Archivists Are Not Alone on the Wild Frontier," *Archivaria* 44 (Fall 1997), pp. 44–71; ICA Committee on Electronic Records, "Guide for Managing Electronic Records"; Paul Marsden, "When Is the Future? Comparative Notes on the Electronic Record-Keeping Projects of the University of Pittsburgh and the University of British Columbia," *Archivaria* 43 (Spring 1997), pp. 158–73; Barbara Reed, "Metadata: Core Record or Core Business?," *Archives and Manuscripts* 25 (1997), pp. 218–41;

Following the 1997 Research Conference

After 1997, the landscape changed substantially. The University of Pittsburgh project formally ended and its team moved on to other matters.[20] Several follow-up projects funded by the NHPRC in Philadelphia, New York State, and at the University of Indiana completed their research over the following years.[21] Essentially these subsequent projects confirmed that it was possible to use the Pittsburgh framework to dictate requirements for local electronic records systems implementations, if it was recognized that the framework was to be understood as a general model, not a specification. In 1998, the Public Record Office of the State of Victoria in Australia launched the Victorian Electronic Records Project, which soon demonstrated the possibility of automatic capture of business process metadata from records – one of the Pittsburgh Project's claims that was least substantiated up to that point by practical experience.[22] In addition, the Victorian Electronic Records Project implemented the archival repository and record retrieval environments envisioned by the Pittsburgh Project. Together with the successful implementations at the University of Indiana, these initiatives effectively demonstrated the viability of the Pittsburgh Project's proposed architectures and metadata reference model.

The University of British Columbia project expanded significantly, taking on a vast number of international collaborators as part of the InterPARES

Heather MacNeil, "Protecting Electronic Evidence: A Final Progress Report on a Research Study and Its Methodology," *Archivi and Computer*, vol. 7, nos. 1–2 (1997), p. 22.

20 Bearman ceased publishing on electronic records. Duff completed her dissertation and moved to other interests. Wallace completed his dissertation and continued to publish on some aspects of the use of electronic records in government but not on the central issues of electronic records management requirements. Cox summarized some of the project findings but did not build on them.

21 See Philip C. Bantin, "Developing a Strategy for Managing Electronic Records: The Findings of the Indiana University Electronic Records Project," *American Archivist*, vol. 61, no. 2 (Fall 1998), pp. 328–64; and "The Indiana University Electronic Records Project: Lessons Learned," *Information Management Journal*, vol. 35, no. 1 (2001), p. 16; P.C. Bantin and G. Bernbom, "The Indiana University Electronic Records Project: Analyzing Functions, Identifying Transactions, and Evaluating Recordkeeping Systems; a Report on Methodology," *Archives and Museum Informatics*, vol. 10, no. 3 (1996), p. 246; and Philip C. Bantin, "The Indiana University Electronic Records Project Revisited," *American Archivist*, vol. 62, no. 1 (Spring 1999 [submitted in 2000]), pp. 153–63; M.D. Giguere, "Automating Electronic Records Management in a Transactional Environment: The Philadelphia Story," *Bulletin of the American Society for Information Science*, vol. 23, no. 5 (1997), p. 17; A. Kowlowitz and K. Kelly, "Models for Action: Developing Practical Approaches to Electronic Records Management and Preservation," *Bulletin of the American Society for Information Science*, vol. 23, no. 5 (1997), p. 20.

22 Victoria Public Record Office, "Victorian Electronic Records Strategy (Vers) Project, Final Report," 1998, available at: http://www.prov.vic.gov.au/vers/pdf/final.pdf (accessed 13 September 2006).

project (now dubbed InterPARES 1) initiated in 1999. Concluded in 2001, it extended the theoretical framework grounded in diplomatic theory, and conducted several "case study" probes "focused on the preservation of the authenticity of records created and/or maintained in databases and document management systems in the course of administrative activities."[23] InterPARES 1 developed a series of activity decomposition models of Authenticity, Appraisal, and Preservation, which identified the data flows required to carry out tasks necessary to ensure and preserve authentic records. It then sought to validate these models in case studies, using responses to questionnaires and more detailed interviews. Reports in 2001 suggested that some aspects of the formal models, particularly the level of detail regarding structural metadata required to support certain activities, and the timing of events in the life cycle of electronic records, needed to be revised in light of experience. Problems relating to how complex and proprietary documents could be preserved were identified as being particularly worthy of greater analysis, and on that basis an extension of the project was proposed. InterPARES 2, initiated in 2002, focussed on

> issues of reliability and accuracy from the perspective of the entire life-cycle of records, from creation to permanent preservation, [particularly] … records produced in complex digital environments in the course of artistic, scientific and e-government activities.[24]

Whether the InterPARES project will return to the problems it identified in its conceptual models in phase 1, or replicate the case studies it attempted there, or attempt to implement its findings in actual software systems, is unclear.

Influenced by InterPARES however, a third major theory-building project, the European Commission IDA Programme Model Requirements for the Management of Electronic Records Project, issued its MoReq Specification in 2001.[25] This was an abstract specification for an Electronic Records Management (ERM) system function or service, built on an entity-relation model. Although the language used suggests a very physical model, its "files" and "folders" are virtual and do not "contain" anything. Indeed, the system it describes is essentially a database for assigning metadata to records, an information retrieval system for managing records according to the assigned metadata, and a particularly secure and tightly managed data environment for

23 See http://www.interpares.org/ (consulted 30 August 2006).

24 Ibid.

25 European Commission IDA Program, "MoReq: Model Requirements for the Management of Electronic Records: MoReq Specification" (2001), available at: http://www.cornwell.co.uk/moreq.html (accessed 12 September 2006).

guarding records from purposeful or accidental change. While this "specification" was not intended to actually drive system procurement, it did influence the first major effort to actually build such systems initiated in the United Kingdom.

The (then) Public Record Office in the United Kingdom, spurred by a national e-government plan requiring most citizen-to-agency communication to be electronic by 2004, launched a series of policy and planning efforts that resulted in requirements for Electronic Records Management Systems for UK government agencies.[26] Its documents together describe (in operational detail) the requirements for a tendered system for electronic records management or recordkeeping. The level of detail, together with the fact that this procurement demonstrated awareness of all the theoretical studies and prior implementations, makes them especially useful for locating areas of agreement between the previous studies. These specifications were designed to reduce risks throughout the life of records; the requirements introduced at various points are particularly good ways of identifying moments of risk, and surfacing the tactics that the Public Record Office thought would best address them. Inherent in such statements, especially in functional requirements,[27] are the criteria for what might be thought of as a successful resolution of the identified risks.

Increasingly strands of activity from outside the archival community have seized the initiative from archivally-led projects over the past decade. The Open Archival Information Systems (OAIS) model from the space science community had an influence on both the Pittsburgh and UBC projects, and has since gained substantial adherence in the digital libraries world in conjunction with the (misleadingly named) OAI Protocol for harvesting "archived" publi-

26 Public Record Office, "Management, Appraisal and Preservation of Electronic Records, Vol. 2, Procedures," 2nd ed. (Kew, 1999), available at: http://www.nationalarchives.gov.uk/electronicrecords/advice/pdf/procedures.pdf; "Requirements for Electronic Records Management Systems, Vol. 1, Functional Requirements" (Kew, 2002), available at: http:// www.nationalarchives.gov.uk/electronicrecords/reqs2002/pdf/requirementsfinal.pdf; "Requirements for Electronic Records Management Systems, Vol. 2, Metadata Standard (Final Revision)," (Kew, 2002), available at: http://www.nationalarchives.gov.uk/electronicrecords/reqs2002/pdf/metadatafinal.pdf; "Requirements for Electronic Records Management Systems, Vol. 3, Reference Document (Final Revision)," (Kew, 2002), available at: http://www.nationalarchives.gov.uk/electronicrecords/reqs2002/pdf/referencefinal.pdf; "Sustainable Electronic Records: Strategies for the Maintenance and Preservation of Electronic Records and Documents in the Transition to 2004," version 1.0 (Kew, August 2001), available at: http://www.nationalarchives.gov.uk/electronicrecords/advice/pdf/preservation_toolkit.pdf; "Management, Appraisal and Preservation of Electronic Records, Vol. 1, Principles" (Kew, 1999), available at: http://www.nationalarchives.gov.uk/electronicrecords/advice/pdf/principles.pdf (all accessed 12 September 2006).

27 Public Record Office, "Requirements for Electronic Records Management Systems, Vol. 1, Functional Requirements."

cations. The efforts of RLG and OCLC, subsequently joined by the US National Archives and Records Administration, in their work on trusted digital repositories, have focussed on managing the social sources of long-term retention risks. Research on emulation and on format migration sponsored by the UK Joint Information Systems Committee, and the US Digital Libraries Federation and Mellon Foundation, among others, has addressed the technical risks of format obsolescence.

In the final section of this paper, we examine how these efforts intersect with a framework for understanding archival risks around which a consensus, if unarticulated, has developed.

Moments of Risk

... the authenticity of electronic records is threatened whenever they are transmitted across space (that is, when sent to an addressee or between systems or applications) or time (that is when they are in storage, or when the hardware or software used to store, process, communicate them is updated or replaced).[28]

A technological boundary exists between any two states of a system or of interoperating systems when the transition from one state to another does, or can, entail significant changes in attributes or methods of a digital object. For records, significant changes are those that affect identity or integrity ... Preservation control is critical in transitions across technological boundaries. Preservation control consists of actions, conditions and constraints designed to ensure the preservation of records and their continued authenticity.[29]

It has become widely accepted that electronic records are at greatest risk of losing their "record-ness" at moments when they are transitioning between states, e.g., when control is being passed to different systems.

... it is possible to track every access to a records system and every action on any record in the system. A system can be designed so that, once filed, a record is never out of file; users get access only to copies of the record. System design can also preclude any

28 Heather MacNeil, "Providing Grounds for Trust II: The Findings of the Authenticity Task Force of InterPARES," *Archivaria* 54 (Fall 2002), pp. 24–42 (quotation on p. 28); InterPARES Authenticity Task Force, "Authenticity Task Force Requirements for Assessing and Maintaining the Authenticity of Electronic Records," *Archivaria* 54 (Fall 2002), pp. 43–58 (quotation on p. 45); InterPARES, "The Long-Term Preservation of Authentic Electronic Records: Findings of the InterPARES Project," Principle 3 (2001), available at: http://www.interpares.org/book/index.cfm (accessed 12 September 2006).

29 InterPARES, *Preservation Task Force Final Report, Draft for Comment* (31 October 2001) pp. 90, at: http://www.interpares.org/documents/ptf_draft_final_report.pdf (accessed 17 November 2006).

alteration or destruction of records except by authorized persons … However, such controls are only effective within the confines of a system. When a record is taken out of a system, or when the system itself is modified, systematic control is at risk.[30]

This agreement on the nature of risk means that the specific states and types of risks, as well as the criteria for assessing whether a transition has been successful could be generally agreed; an appropriate model would expose moments of risk independent from solutions that have been offered to manage them. The framework suggested here builds on a model of the life of an electronic record in which it falls under the control of four discrete systems environments:

- A Creation Environment, where an action results in an electronic document being made and sent;
- An Active Records Management Environment, into which the electronic document is saved or received under the control of an application supporting ongoing use;
- An Archival Environment, where an electronic record, complete with sufficient metadata to ensure its authenticity, has been ingested and is being managed archivally; and
- A Preservation Environment, in which interventions are made by archivists for the purpose of prolonging the useful life of the record.

Within these four environments there are six occasions in the life of documents that are particularly dangerous for the integrity and authenticity of the record. These moments, and the state transitions that create risks, are illustrated in Figure 1 below.

Using this model of the moments of risk encountered in the life of electronic records, and their source in state transitions, particularly across systems boundaries, we return to the literature, where we encounter numerous enumerations of "risks," "problems," and "issues" affecting the management of electronic records, to classify what others have been pointing to. An analysis of these reveals that they are sometimes complete statements of the moments of risk and at other times only partial lists where the remaining risks are identified elsewhere in the same article or report. A substantial database of these statements, linked to moments of risk, was generated in the course of research for this study, from sources such as the UK Public Record Office "Principles for Management, Appraisal and Preservation of Electronic Records."[31] Based

30 InterPARES Strategy Task Force, "Strategy Task Force Report," p. 3.

31 Public Record Office, "Management, Appraisal and Preservation of Electronic Records, Vol. 2, Procedures."

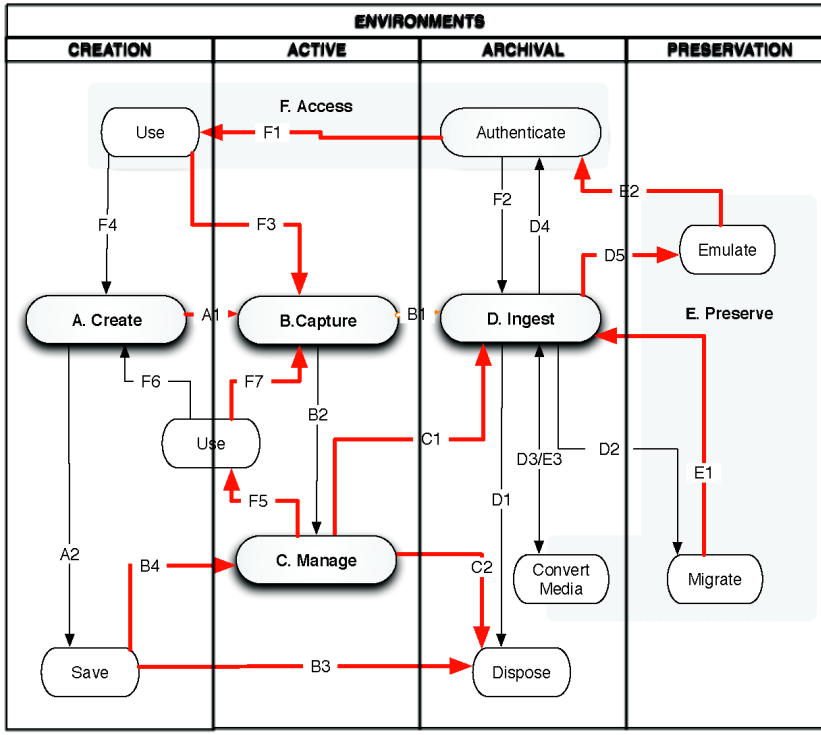

Figure 1: *Boundaries between systems (usually hardware and software, though potentially software only) are indicated by the vertical lines separating the table into four environments. The high risk transitions are indicated by the labelled bolder lines (referenced in the remainder of this text with the notation [Alphanumeric]). Less risky transitions, typically within one system environment or simple exports, are indicated by lighter lines.*

on this index of the positions various researchers have taken, we can explore these moments of risk in greater detail.

Creation Environment

Basically a record can be no more reliable than it was at the instant of its creation ... Authenticity refers to the persistence over time of the original characteristics of the record with respect to context, structure and content. An authentic record is one that retains its original reliability.[32]

32 ICA Committee on Electronic Records, "Guide for Managing Electronic Records," p. 22.

Capture – Content

The first "moment of risk" in the life of an electronic record is at the moment of capture, and determines whether it is saved in the creator's systems and captured in the recipient's system at all, or in the same form [A_1, A_2, B_2]. The literature agrees that when a system creates data reflecting an institutional or individual action, and that data is captured by the sender or recipient in the course of a transaction or communication, a "document" of one or more files or data formats – an email; a database update transaction; a spreadsheet, graphic, or image; a sound or multimedia file – is created. Technically, this document could reside in RAM in the creating system and never have been "saved" [A_2], but a copy of it has to be recorded in the receiving system to be seen [B_2]. To some, whether the document becomes a "record" depends on whether it is then "set aside" – that is, consciously managed – by the sender or recipient. As the InterPARES Project put it, "a record is defined as any document created – meaning made or received and set aside either for action or reference – by a physical or juridical person in the course of practical activity as an instrument or by-product of it."[33]

The Pittsburgh Project envisioned that a record would be ingested into an archive as a consequence of the same action that transmitted it from the creator's system [B_1]. The "set-aside" function was forced to occur by default.[34]

> A transaction is communicated from one physical or logical place to another, whether it is from one person to another, one hardware/software machine to another, or both. As such it crosses a logical switch, and when it does so, it can be captured. What a business considers a transaction, we have called a "business transaction" and the Swedes have more recently dubbed a "causa"… Every time a business transaction crosses such a "switch" implementers will want to create a record of the transaction.[35]

The act of capturing takes place within the sending system and the receiving system independently, but does not create something that must be managed as a record. In the sending system, the saving of a document (but not of a record) is, as a technical matter, essentially risk-free [A_2]. But socially, saving a document can be very risky. The sender may dispose of it rather than "setting it aside" in a management system, or may change it, purposefully or accidentally, prior to "setting it aside" in a management system [B_4]. The capture of the same document within the receiving system involves more risk; normal

33 InterPARES, "Long-Term Preservation of Authentic Electronic Records."

34 In this model documents are captured in archives at the time of their initial transmission, so the copy received by the recipient, and put in active management, no matter how changed, does not threaten the authenticity of the record as evidence.

35 Bearman, "Item Level Control," p. 195.

business practice is only possible because the presumption can be made that what is received is in fact what is sent. But since the receiving system may not have the software required to appropriately render the received document, the presumption that the recipient has in fact "seen" the document *as sent* is not always valid. As it is necessary for the receiving system to write a copy locally in order for the recipient to open it, there will, at first writing, be an accurate copy, assuming successful transmission. But again there is a risk that the recipient may not "set it aside" or may alter it before "setting it aside" [F_3, F_7]. Permitting senders or receivers to determine disposition at this stage [B_3, C_2] is very risky (as is any disposition determination) particularly as there is no schedule or guidance governing the act and the end-user may have interests other than those of the organization.

Capture – Metadata

The largest risk faced by anyone using electronic information systems, and ultimately by records managers, archivists, and those concerned with evidence, is that documents are not, by anyone's standards, the same as records. In order to save a record, the captured document (or trace) needs to be accompanied by adequate metadata relating to content, structure, and context to establish its value as evidence. Both content and metadata need to remain together, unaltered, and usable over time. There is agreement in the literature that systems do not necessarily make records and that there is a major risk, incurred at Capture and again at Ingest, that inadequate metadata may be captured or it might be stored in a way that permits it to be alienated from the record to which it applies.

> In analyzing the live systems, we were specifically concerned with (1) establishing the status of the digital entities contained within them as records and (2) identifying the elements of such records specifically associated with identity and integrity. With respect to (1) we found that a surprisingly large number of the systems examined in the early case study rounds did not appear to contain records when measured against the evaluation criteria established by contemporary archival diplomatics.[36]

> ... few if any information systems existing in organizations create records, or at least records which are adequate to serve as *evidence* of business transactions.[37]

If a document has been captured, the organization or user may wish to create a record. The Pittsburgh Project argued that, for simplification of architecture and functionality, systems should always default to creating a new archival

36 MacNeil, "Providing Grounds for Trust II," p. 31.
37 Bearman and Trant, "Electronic Records Research Working Meeting."

record, bypassing the need for the active records environment to do so [B_1]. Some others have built in an option to exclude certain documents from being stored as records, reflecting a sensitivity towards archival tradition and organizational practice of records management [A_1 ,A_2, C_1, C_2]. Both those who would store everything as a record and then dispose almost instantly of the records that the organization did not, as a matter of policy, wish to keep, and those who would dispose of documents the organization did not wish to keep, and then retain the rest as records, have to face the same two issues:

- For documents or records that are not to be kept, how to ensure that the decision to dispose reflects organizational policy; and
- For records being kept, how to ensure that the records carry metadata reflecting their content, context, and structure adequate to their authenticity and long-term preservation.

Because capture of essential metadata is not typically built into the document creation and transmission process, the fault for failing to create records does not necessarily lie with the record creator/recipient. Often, as the International Council on Archives explained in 1997,

> ... even if one assumes the existence of a high level of motivation to ensure accountability, the very notion of what a record consists of is not as obvious as in the paper world, and the mechanisms for creating it may not be available to the potential record creator unless certain prior actions have been taken.[38]

The continued inadequacy of systems in this respect was recently reconfirmed by the InterPARES project. As Heather MacNeil reported in 2002:

> The case studies revealed that the elements relating to context, in particular to procedural and technological context, were most relevant to an understanding of the electronic record-keeping environment and appeared to provide the main grounds on which creators based their presumption of the records' authenticity [...] for example, in several case studies, audit trails which are considered part of the records' technological context, were identified by the creators as a significant means of ensuring the authenticity of electronic records [...] left unanswered (were) at least two important questions concerning the way in which audit trails functioned in a particular environment: Firstly, what actions taken on an electronic record are recorded and stored in the audit trail? Secondly, what types of information are captured about each action?[39]

As Sue McKemmish and her colleagues explained in 2002,

38 ICA Committee on Electronic Records, "Guide for Managing Electronic Records," pp. 26–27.
39 MacNeil, "Providing Grounds for Trust II," p. 34.

… when records move beyond the boundaries of the local domain in which they were created or, as is increasingly the case in networked environments, they are created in the first place in a global rather than local domain … metadata needs to be made explicit, that is, captured and persistently linked to the record.[40]

In the mid-1990s, John McDonald and his colleagues in Canada had proposed implementing a front-end environment to ensure that documents could be captured with records metadata that reflected their source business processes. But the apparatus proved too burdensome for most users and was abandoned after some prototypes.[41] More recently, Ken Thibodeau reported his attraction to an object-oriented environment that enforced business rules and captured business process metadata with records from the time of their creation. Noting the inadequacies of a separate records management application to serve record-keeping functions, due to the lack of contextual metadata at the point of capture, he stated that:

… the only possibility the [DOD] 5015.2 standard offered for adapting the record-keeping application to specific processes was in those cases where the traditional filing system for paper records was well suited to the business process. In contrast, the approach taken in the DOCT project [the object-oriented environment implemented within the Patent and Trademarks Office] integrated the prosecution of patent applications with the production, receipt and use of records. This integration was readily apparent in the screen display of the "electronic file wrapper"… the wrapper included buttons that the user could click on to launch steps in the prosecution process. The specific buttons that appeared on the wrapper varied, depending on the job of the user.[42]

Finessing the details, the Pittsburgh Project, attracted by versions of both these solutions, argued that functional appraisal prior to the creation of records could generate the necessary metadata to ensure creation of records at Ingest. Alternatively, records managers and registration functions within organizations can assign the necessary metadata during Management.

40 Sue McKemmish, Glenda Acland, Nigel Ward, and Barbara Reed, "Describing Records in Context in the Continuum: The Australian Recordkeeping Metadata Schema," *Archivaria* 48 (Fall 1999), pp. 3–43 (quotation on p. 7); Glenda Acland, "The Australian Recordkeeping Metadata Schema – Version 1.0: Note from the Research Team," *Archivaria* 49 (Spring 2000), pp. 241–47.

41 John McDonald, "Government on-Line and Electronic Records: The Role of the National Archives of Canada," in Bruce Dearstyne, ed., *Effective Approaches for Managing Electronic Records and Archives* (Lanham, MD, 2002), pp. 73–88.

42 Kenneth Thibodeau, "Building the Future: The Electronic Records Archives Program," in Bruce Ambacher, ed., *Thirty Years of Electronic Records* (Lanham MD, 2003), pp. 91–104 (quotation on p. 94).

Active Records Environment

Record-keeping systems are distinguished from information systems within organizations by the role they play in providing organizations with evidence of business transactions (by which is meant actions taken in the course of conducting their business rather than "commercial" transactions). Non-record information systems, on the other hand, store information in discrete chunks that can be recombined and reused without reference to their documentary context.[43]

One of the things the diplomatic analysis highlighted was the extent to which electronic systems are still being designed to manage data rather than records.[44]

The literature agrees that a major risk in the life of records occurs prior to their ingestion into a record-keeping system, or transfer into an archival control environment: they are liable to be altered, to lose their original identity, or to be separated from metadata required to establish their authenticity [C_1]. The solution to the risks entailed in managing electronic records was originally addressed by the author by stating, tautologically, that they must be kept in a "record-keeping" system.[45] A detailed requirements statement for such a system was identified early-on as a way of enumerating the nature of the perceived threats.

Any organization that wants to use electronic documentation as evidence in the future will need to satisfy the requirements of evidence in the normal course of conducting its business. It has been difficult to do so in the computer-based communications environments we have implemented in the past because applications software sold by third parties has not met these requirements. Information systems are generally designed to hold timely, non-redundant and manipulable information, while recordkeeping systems store time bound, inviolable and redundant records. Few, if any, in-house information managers have been able to devote the energy to rigorous definition of the distinct requirements for recordkeeping or, if they had, would be able to envision how to satisfy these throughout all systems. Without such explicit and testable specifications, computing application and electronic communications systems have failed to satisfy the requirements for recordkeeping and are, therefore, a growing liability to companies even while they are contributing directly to day-to-day corporate effectiveness.[46]

Increasingly, the functions of such systems are fully specified in tender documents.[47]

43 David Bearman, "Record-Keeping Systems," *Archivaria* 36 (Autumn 1993), p. 17.
44 MacNeil, "Providing Grounds for Trust II," p. 32.
45 See Bearman, "Record-Keeping Systems."
46 David Bearman and Ken Sochats, "Metadata Requirements for Evidence" (1994), available at: http://www.archimuse.com/papers/nhprc/BACartic.html (accessed 21 September 2006).
47 See the PRO documents cited in footnote 25.

These threats may be related to systems administration, use, and ongoing metadata acquisition or loss. Systems administration threats are, of course, not specific to electronic record-keeping environments, but they pose a fundamental challenge in a system whose entire purpose is to preserve the integrity and authenticity of the records it holds. These threats can be addressed through good systems management practices – backup and recovery, database integrity, sound metadata management, ongoing data conversion, etc. The simplest solution to threats in an active use environment may be the LOCKSS (lots of copies keep stuff safe) approach, but it is not always acceptable in a record-keeping context for reasons of security, privacy, and laws relating to control of records. Crucially, the system should be designed and administered to execute its own rules faithfully; those in the future should be able to trust absolutely that it has done, and that it has kept an auditable record of having done so. As Margaret Hedstrom put it:

> ... trusted systems are defined as systems that can be relied on to follow certain rules at all times. Record-keeping systems are a type of trusted system where rules govern which documents are eligible for inclusion in the record-keeping system, who may place records in the system and retrieve records from it, what may be done to and with a record, how long records remain in the system, and how records are removed from it.[48]

Use-based threats are inherent in the purposes of business information systems – modifiability, non-redundancy, and timeliness. They are managed to the extent that record-keeping systems are non-modifiable, time-bound and redundant, and by the way the system environments enforce rules pertaining to updating.

> Not all data that has been communicated or created by information systems in contemporary organizations is captured as evidence. Information systems are generally designed to hold timely, non-redundant and manipulable information, while record-keeping systems (information systems designed to capture and maintain evidence) store time bound, inviolable and redundant records. Therefore, application environments that support the ongoing work of the organization frequently, or even usually, do not satisfy the requirements for creating evidence.[49]

What happens to records that have been altered is the crucial issue – do they return to the creation process as new documents? Or are the records and all subsequent changes to them somehow maintained through a system of version control within the record-keeping system? The simplest solution – that speci-

48 Hedstrom, "Building Record-Keeping Systems," p. 57.
49 Bearman, "Item Level Control."

fications are increasingly advocating – is to force all copies to return to the system as newly-created documents [F_4, F_6].

For this reason, Bearman and the Pittsburgh Project recommended bypassing the maintenance environment altogether, and sending records directly from capture into record-keeping control.

> Every time a business transaction crosses such a "switch" implementers will want to create a record of the transaction. This record will consist of the content of the transaction encapsulated with metadata, while allowing the data and systems instructions created by the application to be communicated within the information system where it will do the work of the application and be available for further manipulation. In other words, the data in the information system continues to act in the way the application designer intended (updating databases, being available for users to store as information copies, etc.), but from the perspective of the recordkeepers, all data resident in [an] application system becomes a convenience copy, rather than a record, and can be modified under the rules of those systems because the record exists elsewhere, as a separate object, which is not subject to modification.[50]

This seemed quite radical at the time, but a careful reading of the Public Record Office records management functional requirements suggests, that for all practical purposes, they have effectively required the same thing, using a "Records Management System" to control authentic copies in conjunction with electronic office systems, which generate revisions that are recorded as new records. These requirements are summarized in the principle that:

> ... electronic records should be able to function as evidence of business activities and processes … In order to be reliable and authentic they must adequately capture and describe the actions they represent, and once created not be capable of change without creating a new record.[51]

In more detail, the step-by-step requirement for such copy protection and re-insertion into the overall system through the Create function can be found in the statement of requirements for "Move, copy, extract and relate" (sections A2.50–2.62) in the UK Public Record Office "Functional Requirements for Electronic Records Management Systems."[52]

If the metadata that needs to be associated with records to preserve their identity and reliability, and prove their authenticity, is not maintained along with active records, and if changes to records' metadata are not recorded (to

50 Ibid.

51 Public Record Office, "Management, Appraisal and Preservation of Electronic Records," p. 27.

52 See the PRO documents cited in footnote 25.

document ongoing uses, for example), then the records will not have the metadata required when they are transferred to an archive. As Sue McKemmish and colleagues put it,

> ... recordkeeping processes (including archival processes), "fix" documents which are created in the context of social and business activity, and "preserve" them as evidence of that activity in ways that assure their accountability for as long as they are of value. Managing documents as evidence of social and business activity involves developing records and archives systems that can carry them forward with their "fixed" content, render their structure or documentary form, and maintain sufficient contextual links to preserve their meaning through time.[53]

A considerable amount of ink has been spilled over the "need" to maintain electronic filing systems, and keep records in the original order of their record-keeping files. It is important to note however that the actual physical file structures are utterly arbitrary, and the logical files are just that – logical. "Putting" electronic records in files and folders and managing their "hierarchies" is a consequence of classification. As the European Union put it in 2001 (after expending many pages on the virtues of filing systems):

> In an ERMS electronic records can be managed as if they are accumulated in electronic files and stored in electronic folders. Strictly, electronic files and folders need not have a real existence; they are virtual, in the sense that they do not really "contain" anything; in fact they consist of metadata attributes of the records assigned to them.[54]

Archival Environment

Ingest

> A record is a specific piece of information produced or received in the initiation, conduct or completion of an institutional or individual activity. It comprises sufficient content, context and structure to provide evidence of that activity. It is not ephemeral: that is to say it contains information that is worthy of preservation in the short, medium or long term.[55]

When users generate a "Business Acceptable Communication," consisting of content encapsulated by all the metadata necessary to ensure its integrity and longevity, the record should be split off from the application systems environment and sent to a sepa-

53 McKemmish et al., "Describing Records in Context in the Continuum," p. 8.

54 European Commission IDA Programme, "MoReq: Model Requirements for the Management of Electronic Records."

55 Public Record Office, "Management, Appraisal and Preservation of Electronic Records," p. 12.

rate recordkeeping system or API [application programming interface] layer recordkeeping service where it will be kept intact. This means that systems implementers need to construct "traps" in which they can capture the business transaction along with the metadata required for evidence. Most of this data, such as the time of the transaction, the identity of the sender and recipient, and the structural dependencies of the data, can be readily adduced from information available to the application and operating environment. The issue is how to generate, and capture, the metadata which identifies the business transaction-type or task of which the record is evidence.[56]

During ingestion into a record-keeping system, whether by transfer from a management environment [C_1] or at the time of capture [B_1], there is considerable risk that adequate metadata to document content, structure, and context might not be recorded and/or stored irrevocably with the record. The Pittsburgh Project asserted that business process metadata (documenting the broad functional context) and structural metadata (documenting systems dependencies) could be captured automatically from electronic applications environments at the time of record capture.

Indeed, there was every reason to prefer a more conservative option, which placed a record-keeper and "registry" function between the creation and ingestion, and made a traditional assignment of metadata through classification. The theory based on the Pittsburgh Project always left this possibility open, as the italicized statement below makes clear:

The functional requirements for evidence in recordkeeping dictate the creation of records that are comprehensive, identifiable (bounded), complete (containing content, structure and context), and authorized. These four properties are defined by the requirements in sufficient detail to permit us to specify what metadata items would need to describe them in order to audit these properties. This descriptive metadata cannot be separated from them or changed after the record has been created. Several additional requirements define how the data must be maintained and ultimately how it and other metadata can be used when the record is accessed in the future. The metadata created with the record must allow the record to be preserved over time and ensure that it will continue to be usable long after the individuals, computer systems and even information standards under which it was created have ceased to be. The metadata required to ensure that functional requirements are satisfied must be captured by the overall system through which business is conducted, *which includes personnel, policy, hardware and software*.[57]

This option was generally preferred in Europe where registry functions

56 Bearman, "Item Level Control."
57 Ibid.

existed and worked reasonably well with paper records (as predicted[58]) and was the approach adopted by InterPARES.

The Pittsburgh Project, by specifying immediate exercise of archival (or record-keeping) control over records, highlighted the importance of early ingest and the possibility of having metadata assigned by an automatic process rather than a human-mediated one. This point was reiterated by the International Council on Archives, that argued that most record-making decisions be made prior to the creation of individual records. First, the ICA noted that:

> In the electronic environment, however, as with records creation, tasks associated with appraisal and selection must be initiated early in the life cycle, often at the stage of "conception," because retention requirements based upon archival considerations should be built into an electronic system at the time of its design.[59]

The report went on to assert that:

> The conception stage is the most advantageous time for appraisal, because it provides the greatest opportunity for ensuring that appraisal decisions are effectively implemented … Appraisal at the maintenance stage is not desirable. First, there are risks that adequate records will not have been created; that the authenticity of records cannot be demonstrated; that the records are incomplete, unreliable or not interpretable; or that the information that is retained reflects only how an organization carried out its record keeping, and not how the organization accomplished its functions and activities.[60]

In effect, the experience of trying to apply the InterPARES guidelines in case studies also upheld this conclusion. As Heather MacNeil wrote in 2002,

> … the case studies revealed little consistency in the way the attributes that specifically establish the identity of record (e.g., the names of the author and addressee, the indication of the action or matter, the manifestation of the bond linking the record to others participating in the same action) are captured and expressed from one electronic system to another. In many cases, certain attributes (for example, the expression of the archival bond) were not captured at all. This finding underlines the need to make certain of those elements explicit in order to ensure that knowledge of the key indicators of identity is not lost when the records are removed from the specific electronic system and record-keeping environment in which they have been created and actively used.[61]

58 David Bearman, "Diplomatics, Weberian Bureaucracy and the Management of Electronic Records in Europe and America," *American Archivist*, vol. 55, no. 1 (Spring 1992), pp. 168–80.

59 ICA Committee on Electronic Records, "Guide for Managing Electronic Records," p. 27.

60 Ibid., pp. 33–34.

61 MacNeil, "Providing Grounds for Trust II," p. 33.

Looking at a range of actual situations as the Archives of Ontario began to accession electronic records, Jim Suderman noted that:

> The physical proximity of records within the old subject file structure suggests that correspondence may have directly influenced decision-making and policy direction … That comforting (but unsubstantiated) implication disappears with the new case file structure … Similarly, evidence of the relationship between the files themselves disappears with the transition from subject files, governed by a classification system, to numerically ordered case files … The relationship with the functions or activities to which the record relates is what has arguably become less clear in the electronic environment.[62]

Nowhere is the point that the relationship between functions and activities, and the resulting record was obscured by electronic processes more powerfully made than in the ongoing debate over databases. Databases are an information systems application that privileges current and timely data and deprecates record-keeping values. The "records" relating to databases consist of the update transactions (additions, edits, and deletions) and the output transactions (reports, query results, notices triggered by database states, etc.). The database, at any point in time, reveals no evidence of what transactions have updated it or outputs have been generated from it. As the International Council on Archives put it:

> Records from updating transactions should be retained if there is a need for documentation of these transactions as such, or if the retention procedures implemented in the database are not able to retain records that are of business or archival value, before they are altered … Output presentation records should be retained when there is need to document these transactions took place, or when they play a role as evidence in a context outside the database system, for instance as part of a case file.[63]

Unfortunately, this remains an area where there is much confusion about what needs to be controlled in order to ensure authentic records; note, for example, the UK Principles 1.28 and 1.29.[64] As a consequence, the UK "Functional Requirements for Electronic Records Management Systems" do not even provide for capture of database transactions; all issues relating to the authenticity of databases and actions with respect to them are completely neglected, meaning also that records received from such databases by users employing standard database access methods (e.g., querying a database that they have permission to view) are not being recorded at all. Yet the user has

62 Suderman, "Defining Electronic Series," p. 36.
63 ICA Committee on Electronic Records, "Guide for Managing Electronic Records," p. 46.
64 Public Record Office, "Management, Appraisal and Preservation of Electronic Records."

received a copy of a record, and can with appropriate access permission alter or overwrite the state of the record as they found it.

Access

Of course, records also must be protected from change. Regardless of how they are stored, only copies of records should be given out to other systems, and as soon as they are opened they need to lose the validation bits which certify their recordness.[65]

4.5.4 The ERMS must prevent any change to the content of the electronic record by users and Administrators.[66]

Users wish to access records both during their active life [F_5] and after they are declared archival [F_1]. At either time, they require assurance that the records consulted are authentic and unaltered. They may wish to use the records or extracts from them within a context that will produce a new record. Copies created therefore need to be "authenticate-able" and revisable. Yet once revised, copies must clearly indicate revisions; the resulting document must not be able to re-enter the system in any way that might replace the original record or be confused with it.

In response to access requests, producing a copy involves production within one system, and hence no real risk [D_4]. But authentication which involves application of some software rules and/or human judgment [F_1], introduces some risk. The InterPARES project emphasizes a range of methods of verification familiar to those working with paper records:

Methods of verification include, but are not limited to, a comparison of the records in question with copies that have been preserved elsewhere or with backup tapes; comparison of the records in question with entries in a register of incoming and outgoing records; textual analysis of the record's content; forensic analysis of the medium, script and so on; a study of audit trails, and the testimony of a trusted third party.[67]

These methods may be necessary when electronic records that have not been managed are discovered or brought to an archive, but they are clearly less desirable than bringing the authentic record under control at its creation. Therefore, those who have focussed on the design of record-keeping systems, such as the Pittsburgh Project, VERS, and current specifications for Records Management Systems in the UK, have tended towards encapsulated content

65 Bearman, "Item Level Control."

66 European Commission IDA Program, "MoReq: Model Requirements for the Management of Electronic Records."

67 InterPARES Authenticity Task Force, "Authenticity Task Force Requirements for Assessing and Maintaining the Authenticity of Electronic Records," pp. 46–47.

and metadata using more technical means of establishing the unaltered character of a record.

Once a copy has been authenticated it is necessary to ensure that it cannot be altered or returned to the system [F_3,F_7] except through a new act of capture. This seems to be enforced by the record-keeping requirements examined, except in the case of databases where requirements for authenticating record and transactions seem to have been completely neglected.

Dispose

Not all electronic documents which are created are appropriate to be filed as records; some are purely ephemeral or personal, some merely contain a re-iteration of information held elsewhere.[68]

3.4.6 The ERMS must prevent the deletion of an electronic file or any part of its contents at all times with the exception of: destruction in accordance with a retention schedule … deletion by an Administrator as part of an audited procedure.[69]

Disposal always involves some risk, as an irreversible decision must be taken to execute a schedule, either automatically or by human determination, based on recorded metadata or observable attributes of the records. Some approaches allow for disposal of electronic documents before "becoming" records [B_3], while others deny that possibility and manage everything by retention schedules [C_2, D_1]. Both approaches have difficulty coping with the mixture of personal records in corporate systems and the mixed character of some communications.

Once under records management control, or in a record-keeping system, the scheduling of records disposal is enforced. Some approaches envision the function as one of disposing of files or folders (e.g., aggregations of records with the same file-level metadata) in which case they need to make allowance for the occasions when an individual record must be separated from the file or folder for ongoing retention, as the UK Public Record Office Specification states in sections A.4.14–A4.15, A.4.31, and A.4.40–42.[70] Other approaches envision the disposal of individual records, in which case they must allow for a simultaneous action on numerous records with the same file- or folder-level metadata.

Both approaches are challenged by the need to ensure that all copies of

68 PRO, "Management, Appraisal and Preservation of Electronic Records, Vol. 1, Principles," p. 20.

69 European Commission IDA Program, "MoReq: Model Requirements for the Management of Electronic Records."

70 PRO, "Requirements for Electronic Records Management Systems, Vol. 1, Functional Requirements."

records are subject to disposition. The UK Public Record Office Guidelines state:

> Records management standards on retention and scheduling should apply to electronic records as much as to conventional records. Corporate guidance should aim to ensure that electronic records which possess the same functional and documentation characteristics across the organization are retained for the same length of time, and are disposed of in the same way. Care should be taken to ensure that all copies of an electronic record are brought within this framework, including duplicate copies stored in different locations, and electronic records from which a paper filing copy has been taken.[71]

However, no one has proposed a method by which all copies of records – especially those that have been printed out – could be identified. In systems that are interconnected, automatic comparison is straightforward, but some electronic systems and all paper systems will be outside the control of the record-keeping environment. No practical solution to this dilemma has been found and it remains a major risk in control over disposition.

A second risk is that archivists will know less than they must about records after disposition. The minimum requirement is to know which records have been destroyed under what authority, when, and by whom, but more severe requirements include knowing when and how records were used before they were destroyed – for reasons of liability or ongoing responsibility for administrative control (as in the cases of national security records or some medical records). The Reference Model for Business Acceptable Communications addressed this problem:

> When records are "deleted" under records retention schedules, the contents of the record and the structural metadata and terms and conditions of access and use are destroyed, but the handle, context and use history are not, and a final transaction is added to use history to document the rules under which the disposal took place. When records are incorporated into other records, the terms and conditions for disposal of the parent record govern the incorporated records, but the terms and conditions for access and use in the original records still apply to their use within the subsequent transaction. When records are released under restricted terms and conditions, either because access to them is limited to a specific class of people or because view or use restraints are placed on released copies, the use and user are recorded in the use history of the record being released in addition to the actual content released being incorporated into a new transaction record.[72]

71 PRO, "Management, Appraisal and Preservation of Electronic Records, Vol. 1, Principles," p. 30.

72 David Bearman, "Towards a Reference Model for Business Acceptable Communications,"

Since then, similar requirements have been specified by the MoReq:

5.3.15 The ERMS must have the ability to retain metadata for files and records which have been destroyed or transferred.[73]

Preservation Environment

Preserving a record's authenticity is predicated on its endurance and stability over time … This finding requires that we re-think our reliance on the notion of an unbroken chain of custody as a guarantor of record authenticity … as the Preservation Task force points out: "Given that the storage and retrieval processes for electronic records inevitably entail physical and representational transformations, the traditional concept of an unbroken chain of custody needs to be expanded to encompass the processes that are necessary to ensure that an electronic record is transmitted over time without inappropriate alteration." The Preservation Task Force calls this expanded principle the unbroken "chain of preservation."[74]

Archival preservation requires that … transformations respect the authenticity of the records and that such changes enable the records to be retrieved and understood. Such transformation must be thoroughly documented.[75]

Perhaps the greatest risk to electronic records is that no certain methods have been developed to ensure that they can be preserved over time. While it is a requirement that the records must remain under the control of an archival record-keeping system at all times, the reality is that all the methods we have for preserving the records, except those employed solely to convert media, require that software external to the archival record-keeping system be employed, either to migrate data formats [E_1] and/or to emulate operating environments and applications systems [E_2]. The transition to new formats, and/or media, and the construction and validation of emulation environments, takes place in another system, across a control boundary that signals a moment of risk. Migration of formats and emulation of systems depend on tests for accuracy and completeness that rely on human judgment, entirely outside the control of systems. Because preservation carries risk of loss of authenticity – through loss of metadata, changes in renditions, and, even, loss

1994, Web published proposal, at: http://web.archive.org/web/19970707064048/ http://www.lis.pitt.edu/~nhprc/prog6-5.html (accessed 30 August 30 2006).

73 European Commission IDA Program, "MoReq: Model Requirements for the Management of Electronic Records."

74 MacNeil, "Providing Grounds for Trust II," p. 27; see also InterPARES, "The Long-Term Preservation of Authentic Electronic Records," Appendix 6, "How to Preserve Electronic Records," at:. http://www.interpares.org/book/interpares_book_o_app06.pdf (accessed 21 September 2006).

75 ICA Committee on Electronic Records, "Guide for Managing Electronic Records," pp. 34–35.

of content – there has been a growing agreement that the original bit-stream should simply be kept along with migrated formats as a kind of double insurance, given that the costs of storage continue to drop in accordance with Moore's law. One result of this consensus is to lessen the stridency of the either/or debate over emulation and format migration, since both approaches can be taken for insurance (and advocates of both strategies welcome diversity, aware that there are risks in either approach).

In addition, over the past eight years, migration objectives have become more broadly endorsed and more explicitly identified. As the UK Public Record Office put it in 1999:

> Organizations will need to identify or develop standards for electronic record formats and for the transfer of records, including both preservation and presentation. Several constraints limit the selection of these formats:
> - Minimizing the risk … of becoming locked into proprietary formats and applications
> - The number of formats needs to be limited to minimize the number of migration paths to be managed …
> - The selected transfer formats should require minimal enhancement to a department's normal IT applications.[76]

These objectives may best be met if the first steps towards format migration are taken at capture, and again at ingestion, so the preservation action is, like so much else in electronic records, carried forward in the records life cycle. Indeed, planning for which proprietary formats will be initially captured in what standard formats, and identifying which standard formats will be migrated on ingestion to more widely adopted or resilient standards, takes place at the "conception" stage, prior to the creation of any records. Some promising developments in this area have been reported recently.[77]

Conclusions

Although a variety of conflicting tactics have been put forward to manage electronic records over their life from initial transmission to long-term preservation, the archival literature of the past ten years – theoretical journal articles,

76 PRO, "Management, Appraisal and Preservation of Electronic Records, Vol. 1, Principles," p. 46.

77 Donald S.H. Rosenthal, Thomas Lipkis, Thomas Robertson, and Seth Morabito, "Transparent Format Migration of Preserved Web Content," *D-Lib Magazine*, vol. 11, no. 1 (January 2005), available at: http://www.dlib.org/dlib/january05/rosenthal/01rosenthal.html (accessed 21 September 2006). For progress on a major multi-institutional effort to create an infrastructure for format migration, see Stephen Abrams, Stephen Chapman, Dale Flecker, Sue Kreigsman, Julian Marinus, Gary McGath, and Robin Wendler, "Harvard's Perspective on the Archive Ingest and Handling Test," *D-Lib Magazine*, vol. 11, no. 12 (December 2005), available at: http://www.dlib.org/dlib/december05/12contents.html (accessed 21 September 2006).

reports of working groups, and concrete specifications for systems procurements – is in agreement about the events in the life of electronic records and archives constituting "moments of risk." There is also some agreement in the literature about what aspects of the record need to be protected. There seems to be substantial agreement about the tests that one would apply to determine if records have successfully transited these moments of risk.

Where there are major differences still, they are the result of choosing different tactics to overcome known points of risk. The most significant of these is the risk of maintaining records while providing on-going use of information systems designed for effective administration. The Pittsburgh Project recommended the radical separation of these functions by ingesting records into record-keeping systems simultaneously with their creation, and leaving *in situ* information systems to function without serving any record-keeping functions. In this way new actions always generated records in the record-keeping system, and use copies in the active systems of offices were simply for use. The UBC Project recommended policies and practices in offices with active electronic records systems that would strengthen record-keeping practices until the transfer of records to the archive.

The primary direction of movement since 1997 has been a hybrid. Reports from InterPARES and the European Union, and specifications from the UK Public Record Office and the US National Archives and Records Administration, have called for implementing record-keeping systems within offices with active records. The purposes of these record-keeping systems have been to capture records as close as possible to the moment of creation, but to keep the traditional role of the office of origin as the source of transfers of records to archives after their active life has ceased. The hybrid reflects some legal traditions and practical power relations between agencies of government and the archives. It also effectively recognizes the moments of risk in the management of records and increasingly imposes control so that copies of records and versions of records are effectively captured as new records within these systems.

A second major tactical difference persists in how best to address the risks of preservation. Again hybrid solutions have been adopted in the practical large-scale specifications issued by the National Archives in the US and UK. While early format transformation (at the points of capture and ingestion) has been specified, retention of the original bit-stream as insurance has also been advocated. Work on emulation is still going forward, particularly for operating systems and other widespread dependencies. Together, keeping original bit-streams, and the emulation or migration of proprietary and unusual formats to more standard and stable formats, serve as the best combination of tactics for overcoming the risks of preservation.

A third area of tactical differences relates to the treatment of personal and ephemeral business documents in electronic communications environments. The hybrid solution that has evolved is to capture most documents into record-

keeping systems as soon after creation as possible, to build into systems as much as possible the ability to recognize records from documentable business processes and systems, and to acknowledge that we have no way to identify all non-record material by automatic means. Given this shortcoming, some approaches would err on the side of capturing everything and disposing of non-record material as soon as practicable, while others would err on the side of capturing only what users treat as a record (set aside). In the first case, the risk is of over-retention, while in the latter case it is of failing to keep what should have been retained.

Overall, the past ten years have seen significant convergence on the nature of risks to authenticity. As a consequence, it is possible to identify common criteria – articulated by numerous writers and projects – for assessing the success of approaches taken to reduce these risks. With such common criteria, the heat surrounding the choice of approaches can be reduced; we can begin to judge strategies by how well they achieved agreed objectives rather than by whether they appear to be argued from ideologically correct premises. This seems a major step forward, and lays the groundwork for the development of methods that operate uniformly as network utilities and are supported by an international certification body to ensure the least possible loss in overcoming moments of risk and the longest plausible periods of preservation.[78]

Unfortunately, the largest and best-funded developments in digital archiving are no longer being driven by the archives community. As a consequence of a growing interest in digital preservation within the library community, the term "archiving" and the thrust of most digital preservation research have been diverted to deal with keeping digital objects in library-like repositories. In this context the initial capture of the record as it was originally created and transmitted is typically not an issue and the authenticity of the user-delivered archival record is generally not a matter of legal significance. Hence two of the greatest moments of risk, at capture and access, are outside the scope of many "archival preservation" models.

The International Federation of Library Associations (IFLA) has recently published an excellent review of the state of library-oriented research in digital preservation. When read in the context of the "moments of risk" analysis, it illustrates how important the perspective of archives as organizational records could be to identifying critical system boundaries in the life cycle of evidentiary records.[79] In the library-community digital preservation projects,[80] the

78 David Bearman, "Addressing Selection and Digital Preservation as Systemic Problems," presented at the UNESCO Conference "Preserving the Digital Heritage: Principles and Policies," Den Haag, 4 November 2005. In press.

79 For a recent overview, see Ingebord Verheul, "Networking for Digital Preservation: Current Practices in 15 National Libraries," *IFLA Publication* 119 (Munich, 2006).

80 Planets (Preservation and Long-term Access through Networked Services), Nestor (Network

emphasis has been on the construction of trusted repositories, federated archives, and ensuring long-term access. While these are important questions in keeping and delivering archival records, these largely finesse issues associated with ensuring the initially ingested object is a record, or methods for capturing evidential metadata.

For example, since its initial proposal by the space science community, the OAIS model has attracted archival attention as a useful framework for understanding electronic records. Both the Pittsburgh Project and InterPARES referenced OAIS and employed some of its basic concepts. But the current major implementations of the OAIS model at Los Alamos have supported the highly successful work that originated there with physics pre-prints and digital libraries of published articles. Most recently, Herbert Van de Sompel and his colleagues have been publishing about aDORe (a modular standards-based Digital Object Repository)[81] that stores compound objects (content + metadata encapsulated) as a basis for inter-repository interoperability of archived content. This work has been influential in library digital preservation circles. However, it does not address two concerns of the archival community: it makes no explicit reference to how the objects get compounded or when (e.g., the risks of initial capture), nor does it explicitly address the authenticated delivery of migrated or emulated objects.

Nevertheless, some issues of importance in both contexts are now being addressed directly. The JHOVE project (JSTOR/Harvard Object Validation Environment),[82] is considering how to definitively identify a format dependency and how to validate a migration routine, both major risk factors in determining when objects need to be migrated. If this project goes on to create a range of validated format migration tools, objects with dependencies on particular file formats can be identified and scheduled for migration across any archives holding them, thereby making a substantial contribution to reducing migration risks.

---

of Expertise in Long-Term Storage of Digital resources), kopal (Kooperativer aufbau eines Langzeitsarchivs digitaler Informationen), PROTEAN (Preservation Over Time by Electronic Archiving and Networking), all reflect the library emphasis in digital archiving in which the challenges are seen less as risks within the life cycle of the object than as a challenge of preserving an object, once obtained. As a consequence, most of the moments of risk are invisible – outside the time frame and life cycle of the object within the library.

81 Jeroen Bekaert, Xiaoming Liu, and Herbert van de Sompel, "Representing Digital Assets for Long-Term Preservation using MPEG-21 DID," Los Alamos National Laboratory (LA-UR-05-6878), submitted to DCC Symposium: Ensuring Long-term Preservation and Adding Value to Scientific and Technical Data (PV 2005), Edinburgh, 21-23 November 2005; and "aDORe, A Modular and Stands-Based Digital Object Repository at the Los Alamos National Laboratory," Joint Conference on Digital Libraries (JCDL) 2005, Denver, Colorado, 7–11 June 2005.

82 See http://hul.harvard.edu/jhove/ (accessed 30 August 2006).

Further work must address these moments of risk directly. Articulating the problem as one of the loss of control at transitions across systems will reinsert some archival challenges into ongoing digital preservation studies and implementations.