InterPARES 3 Project
International Research on Permanent Authentic Records in Electronic Systems
TEAM Canada

Title:	Case Study 10(3) – University of Victoria Office of the University Secretary - Policies, Procedures and Tools for E-mail Management and Preservation in a Governance Unit: Workshop 03 Action Item 24 – Framework for Trusted Digital Environment
Status:	Final (public)
Version:	1.3
Date Submitted:	May 2009
Last Revised:	May 2013
Author:	The InterPARES 3 Project, TEAM Canada
Writer(s):	Donald C. Force School of Library, Archival and Information Studies, The University of British Columbia Leah Pearse School of Library, Archival and Information Studies, The University of British Columbia
Project Unit:	Research
URL:	http://www.interpares.org/rws/display_file.cfm?doc=ip3_canada_cs10-3_wks03_action_24_v1-3.pdf

Document Control

Version history			
Version	Date	By	Version notes
1.0	2009-04-02	D. Force, L. Pearse	Discussion draft prepared following identification of action items for CS10(3) at TEAM Canada Plenary Workshop 03.
1.1	2009-05-25	D. Force, L. Pearse	Edits based on feedback from J. Morrison.
1.2	2010-04-30	R. Preston	Corrected document title.
1.3	1013-05-2013	R. Preston	Minor copy content and copy edits.

Action 24: L. Wilson and J. Morrison, with assistance from the Graduate Research Assistants assigned to case study 10(3), to develop a framework for a trusted digital environment based on the Canadian "Electronic Documents as Documentary Evidence Standard" [CAN-CGSB-72.34-2005].[1]

Introduction

At the November 2008 InterPARES 3 TEAM Canada Plenary Workshop, the participants discussed what infrastructure archives require for ingesting and preserving e-mails. This discussion arose from the case study involving the University of Victoria (UVic) Office of the University Secretary (USEC), but the resulting action item applies to more than USEC's specific situation. Like many other archives, the University of Victoria Archives will not have the capability to ingest and maintain control of e-mails in electronic format in the foreseeable future, but this line of investigation will establish what framework is needed to preserve e-mail in a trusted digital repository (TDR).

In January 2009, D. Force met with L. Wilson and J. Morrison. They discussed whether the University Secretary Office's local area network (LAN) could serve as a trusted digital repository (TDR). As mentioned at the November 2008 InterPARES 3 TEAM Canada Plenary Workshop, the parameters of the TDR would be based on the Canadian "Electronic Documents as Documentary Evidence Standard." This document outlines the initial findings of that examination. In order to make the report more applicable to USEC, the report has been augmented by information obtained by L. Pearse who, from March-April 2009, interviewed USEC staff regarding how they manage their e-mail attachments.

Report

One of the first questions to consider for this action item is *why use the Local Area Network (LAN) to preserve e-mails?* As previously noted, UVic Archives currently has no control over how these messages are managed, saved or deleted within the University Exchange

[1] InterPARES 3 Project, "TEAM Canada Plenary Workshop #03: Action Items and Decisions," 4.

server.[2] However, if USEC employees saved their e-mail messages to the LAN and the Archives was given access privileges to these locations, then the Archives may:

1) have better control over the long-term preservation of the messages (than if they remain within the e-mail client); and

2) find it easier to apply retention/disposition schedules to the messages (than if they remain within the e-mail client).

Additionally, if USEC employees save their e-mail messages to the LAN, then two other possible actions may occur:

1) space may be freed up on the Exchange server, thus increasing the operating speed of the system and its response rates; and

2) the number of messages in employees' inboxes would be decreased, thereby reducing the amount of time spent sorting through and retrieving messages, and thus increasing productivity rates.

The LAN is regularly used by USEC employees, but, currently, only some USEC employees use the LAN as a location to save attachments. No evidence suggests that USEC employees save e-mail messages either with or without attachments to this location. In other words, some staff members may download attachments and save them to the LAN separately from the original e-mail message, though this is an idiosyncratic practice unmitigated by best practices or guidelines.

Amongst other considerations, the LAN will need to fulfill requirements prescribed by the Canadian "Electronic Records as Documentary Evidence" standard (CAN/CGSB-72.34-2005) before being transformed into a TDR. "Electronic Records as Documentary Evidence" is a standard to "enhance [electronic records] admissibility as evidence in legal proceedings."[3] The document emphasizes the Canadian "Best Evidence Rule" that reads:

> Despite any rule to the contrary, an electronic court document is admissible in evidence unless, on cause shown before the court, the court has reason to doubt the integrity of the electronic court document, either because reliable encryption

[2] "Case Study 10(3) – University of Victoria Office of the University Secretary - Policies, Procedures and Tools for E-mail Management and Preservation in an Administrative Unit: Workshop 02 Action Item 35 – Implementation of the Directory Records to the University Secretary Office's E-mails."; "Case Study 10(3) [...]: Contextual Analysis"; "Case Study 10(3) [...]: Records Research Questions"; and "Case Study 10(3) [...]: Recordkeeping Research Questions."

[3] Government of Canada, "Electronic Records as Documentary Evidence," CAN/CGSB-72.34-2005 (Gatineau, Canada: Canadian General Standards Board, 2005), vii.

> techniques were not used to support the making of the electronic court document or for another reason.[4]

In other words, if e-mail is not printed, but rather is saved to the LAN and deleted from the Exchange server, the copy on the LAN *will* have to qualify as authentic evidence in a court of law. For this to happen, both the records within the system and the system itself need to have integrity and authenticity.[5]

According to the standard, *integrity* is defined as:

> (of records) reliability and trustworthiness of records as copies, duplicates or comparable representations of electronic records; and reliability and trustworthiness of the RMS in which it was recorded or stored to produce reliable and trustworthy copies and duplicates of electronically stored records.[6]

The "Electronic Records as Documentary Evidence" standard defines *authenticity* as a "property that ensures that the identity of a subject or resource is the one claimed."[7] It also outlines, that an electronic record can only be admissible as documentary evidence if it is deemed to be authentic and is what it purports to be. Furthermore:

> Authenticity requires proof that a document actually comes only from the person, organization, or other legal entity asserting to be its author or authorizing authority.[8]

This statement raises several important questions when considering the LAN as a TDR. Foremost, can such "proof" be determined from documents residing on the LAN? What degree of granularity of metadata is necessary to assert authorship of records on the LAN? If messages are transferred from their originating environment (the Exchange server) and placed in a new environment (the LAN), how is their authenticity affected? Transferring records from one system to another is a migration process and will inevitably affect their completeness. To safeguard the records and ensure that only an acceptable amount of data are lost during migration,[9] the LAN and its files will need to be regularly tested, validated, and signed-off by all stakeholders.[10]

[4] "Evidence Act," [RSBC 1996] Chapter 124, section 41.4 (http://www.bclaws.ca/Recon/document/freeside/--%20e%20--/evidence%20act%20%20rsbc%201996%20%20c.%20124/00_96124_01.xml).
[5] "Electronic Records as Documentary Evidence," 15.
[6] Ibid., 9.
[7] Ibid., 5.
[8] Ibid., section 5.2.2, page 15.
[9] Duranti, Luciana, "The Impact of Digital Technology on Archival Science," *Archival Science* 1, no. 1 (March, 2001), 47.
[10] "Electronic Records as Documentary Evidence," section 6.4.6, page 23.

Other questions impacting the authenticity and admissibility of the records include whether saving e-mails to the LAN would be considered as the "ordinary course of business," or, perhaps more importantly, how consistently would this practice have to occur throughout the organization to be deemed as such? Procedures would need to be developed to establish this practice as the ordinary course for executive offices and compliance would have to be continuously monitored. USEC employees do not currently save their messages to the LAN, but e-mail attachments are often saved to this shared drive. At present, there are no best practices or guidelines in place that could be adapted for managing e-mail messages on the LAN. If the LAN is to become a TDR, additional policies, best practices and guidelines would need to be developed to ensure consistency in matters such as naming conventions and version control.

E-mail migration from the Exchange account to the LAN also poses another issue—loss of quick reference metadata, such as the To/From, date Sent/Received, message size, and if the message has an attachment. This is a concern because if such visual reference information is lost, it is unlikely that staff will refer to the message on the LAN as the primary record. In fact, they may find keeping the e-mail in the e-mail client a better solution than the LAN in such cases. Although it could be foreseeable that staff may only use the LAN for inactive messages, a records management policy would have to clearly define these practices.

Despite these concerns about ensuring the authenticity of the messages, one also needs to consider the authenticity of the system in which they would reside. Section 5 of the "Electronic Records as Documentary Evidence" document stipulates that:

> The electronic record provisions of most of the evidence acts state that where the best evidence rule applies to an electronic record, it is satisfied by proof of the integrity of its electronic records system. Therefore, proof of the integrity of an electronic record is established by proof of the integrity of the [records management system] that recorded or stored it (5.2.3).[11]

In other words, a record residing in a records management system is only as trustworthy as the system itself. This section raises several important questions that need to be addressed by UVic's University Systems office (formerly known as Computing and Systems Services). The University Systems office will need to provide information regarding how it backs up the LAN and provides a backup log.[12] To guarantee the security of the system, the University Systems

[11] Ibid., 15.
[12] Ibid., 26.

office will need a security policy that “include[s] notification of, and protection against, unauthorized access as well as guidelines on access and changes in personnel with access.”[13] In fact, a Security policy is in the later stages of being drafted and is expected to be approved in September 2009 by the Board of Governors. The Archives has had input on the policy. UVic has one existing related policy, called the “Responsible Use of Information Technology Services,” though this focuses on the user and information technology use at UVic, not the “back end” policy that accounts for how use is tracked. In addition to monitoring users, date and time stamps are an important component of the system and procedures “for the regular checking of computer system clocks for accuracy concerning date and time keeping should be documented.”[14] Finally, a quality assurance program (QAP) will need to be implemented to “monitor and judge the records management system.”[15]

One of the foremost questions is how to account for and track record disposition. Can the destruction of e-mails on the LAN be documented? The standard states that an “organization shall be capable of documenting a disposal when proof of destruction is warranted or required based on business, legal and audit requirements.”[16]

Undoubtedly, these are just some of the issues that must be discussed when creating a trusted digital environment for electronic records. Not only is it important that the records themselves be carefully managed to ensure their authenticity over time, but the system in which they reside must also be monitored and considered trustworthy. Only when both criteria are satisfied may the electronic records have a stronger chance of being used as evidence in a Canadian court of law.

[13] Ibid., 27.
[14] Ibid., 28.
[15] Ibid.
[16] Ibid., 25. Also see section 8 (pp. 29-32) for more information on audit trail requirements.