POST-EDRMS: FROM THE DIGITAL CONTINUITY TO THE ARCHIVES. THE CHALLENGES FACED IN INFORMATION MANAGEMENT IN THE DIGITAL ERA

Lale Özdemir– Asst.Prof.Dr., Deputy Head of Information and Records Management Department
(University of Marmara, Istanbul, Turkey)

This article examines the challenges faced by organizations in the digital era with regard to new and changing information management and archival processes and practices.
Key words: Post-EDRMS, digital Continuity, digital information, archival processes, information management.

The digital age has without a doubt drastically changed the nature of information management and has ensured that practices in relation to the management of digital information have changed or are in the process of changing in order to meet the needs of the new digital landscape. In contrast to paper records, digital information and records need to be managed at the onset, at the beginning of the lifecycle, to ensure the continuity and later preservation of information. As is universally known, the archivist's goal is to acquire and preserve archival materials and to ensure they are available to be used as evidence and as information [1, p. 97]. However, ensuring the continuity and preservation of digital information is a completely different ball game to that of preserving paper records. The digital information landscape poses challenges that were, up until recently, either not relevant or not a reality. The digital landscape is both friend and foe when it comes to the management of digital information as challenges such as access to huge volumes of information captured in systems, balancing the information rights of the citizen with ensuring that both sensitive personal and official information is safeguarded are now a reality. These can be considered to be non-trivial records management challenges in the digital age in addition to the following; unexpected consequences of search and search engines on discovery; ensuring adequate context to be able to understand the information being accessed sharing and re-use in the world of open and big data; and defining the roles, responsibilities and behaviour of information/records creators and consumers [2].

All of the above factors should be considered within the context of an increased appetite for transparency and accountability for information. This not only applies to governments releasing information as a result of Freedom of Information Act requests but also applies to archival users who want-even demand- access to archival material of all kinds from the comfort of their computer, while at home or while out and about. It could also be argued that the great strides made in providing digital content in the commercial marketplace decrease the general public's patience for the slower pace made by archival institutions in placing their archival materials online [3].

It is the case that the non-trivial records management challenges prevalent in the digital space have not only impacted on the processes and considerations

© *Lale Özdemir*

Scanned with CamScanner

shaping the management of digital information, shortly to be discussed, but have also ensured that information is now recognised as an asset globally. It took several high Profile examples of data loss in public bodies to highlight the importance of information in its own right and for it to be treated as an asset. In 2008, the year in which the UK government issued compulsory guidance on data handling for public bodies, it was revealed that a public official was sacked or reprimanded virtually every single working day for losing data or breaching protection rules [4].

The use of Electronic records/document management systems (EDRMS) [5, p. 140] is now more common place than ever before but capture into an information management system is just the beginning in terms of the management of digital information. The first stage that will contribute to information being preserved for the future is identifying the information assets an organisation holds. Information assets can range from a database of contacts used by a government body to specific files stored in an EDRMS about the construction of a new highway in a given town. An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently [6].

If an organisation is not aware of its information assets then it is unable to protect them and this also extends to knowing what information you hold so that you can potentially preserve it in the future. Information held by organisations should also be documented because keeping a live document of information assets ensures their contribution and value to the business requirements of the organisation can be assessed on an ongoing basis. Once the identification of information assets and their owners (those employees responsible for the information asset) has taken place, the next step is to consider the issue of digital continuity. Digital continuity relates to the ability to be able to use, open and work with your digital information for as long as you need and in the way in which you need. Digital continuity is vital to an organisation, be it in the public or private sector, because it helps ensure that you operate accountably, legally, effectively and efficiently and thus helps to protect your reputation, make informed decisions, avoid and reduce costs, and deliver better public services [7]. Taking digital continuity seriously means that not only information that is required for business use is protected, but that information is more likely to survive to be transferred to an archive or place of deposit in the future when it is legally required to be transferred, if chosen for permanent preservation. Digital continuity is put at risk when the organisation, management processes or technology of an organisation changes. Digital continuity involves the formulation of policies across different business units of an organisation to ensure that information remains useable over time and is essentially about managing the risk to information. Typically, the following may be implemented in an organisation to help information useable for as long as needed:

1) Appointment of a Senior Risk Officer (SRO) to take responsibility for digital continuity. 2) Establishing the scope and priorities for digital continuity across the organisation. 3) Setting up a team of experts in IT, IM, IA and change management to help manage continuity. 4) Making sure that all relevant individuals across the

Scanned with CamScanner

organisation, including managers in the IT, IM, IA and business change functions, understand digital continuity and their responsibilities in exploring the issues [8].

In terms of managing risk to the usability of digital information, one of the practical steps that information Professionals in organisations can take, is to use a file Profiling tool that provides information such as the age, size and last modified date of files as well as their formats [9]. Crucially, such software Profiling tools help organisations to reduce duplicates of files and also help with long term planning for records that will be transferred to an archive by ensuring that file Profiles that cannot be soundly preserved in the long term are identified and converted to other acceptable formats. An ideal solution is for organisations to not capture records in file formats that are not currently accepted by archives. The implementation of digital continuity for information within information management systems is an ongoing process, as explained above, and should run in tandem with archival processes such as the appraisal and selection and transfer of born digital information. This brings us to the challenges of such practices in the digital information space. The appraisal and selection of born digital should be carried out as soon as possible after creation. Digital information is more vulnerable and therefore, as opposed to those for paper records, the appraisal and selection processes needs to be undertaken early to highlight information worthy of permanent preservation. In order to achieve this, records and information managers within organisations needs to have a clear grasp of which information is needed for business use (information assets), where the information is stored (technical environment) and finally, what the purpose of the information is (business needs).

Information stored across all digital sources should be included within such processes (EDRM systems, collaboration systems, email systems, intranet, internet, social media etc.) and the technology used and any interdependencies between systems should be clearly understood. It is also important to highlight that the implementation of the selection methods used for paper records do not comfortably transfer to born digital information. Any given EDRMS contains thousands of thousands of files which renders the traditional approach of file by file review used for paper void. The selection for digital information should ideally be carried out on a macro basis but this also raises the issue of the sensitivity of digital information. Sensitivity review and the likelihood for error is a risky business as sensitivities in huge volumes of digital information may be difficult to identify without the use of data mining or text mining tools, which as yet, are not widely employed in organisations to assist with sensitivity review. It is almost impossible for a reviewer to sensitivity review files one by one and this highlights the need for the creator of files and records to mark the sensitivities of the information they are dealing with, using the metadata built into systems such as EDRMS. The practice of transferring born digital records to archives although not rare, cannot as yet be considered to be everyday business. Most countries are yet to carry out the transfer of digital records to their archives or are in the process of building digital repositories for transfer that are able to take a multitude of records regardless of complexity of format or media. An interim solution could be the use of current IT

Scanned with CamScanner

systems used with unique business processes layered on to ingest records. The born digital records of many administrations across the globe are about to reach the age of legal transfer to archives and in the absence of digital repositories that provide full digital capability, the national footprint of the interaction between state and citizen may only be partially preserved if digital preservation is not undertaken. Crucially, the implementation of EDRMS is the beginning of a long journey to the archive that is sometimes lined with risk and complexity.

References

1. Laura Miller, Archives: Principles and Practices. Facet Publishing, First Ed. London, 2010, 256 p.
2. Julie McLeod, Access to information: Challenges and opportunities for the records Profession. In: 7th Conference on Scientific Archives, 24 - 26 June 2015, Rio de Janeiro. Retrieved from http://nrl.northumbria.ac.uk/25700/.
3. D. Boyd, Achieving the promise of oral history in a digital age. Ed. D. A. Ritchie. In The Oxford Handbook of Oral History. Oxford University Press, USA, 2010: 287-302.
4. One official disciplined over data loss every day. The Telegraph, 3rd November 2008. Retrieved from http://www.telegraph.co.uk/news/3374341/ One-official-disciplined-over-data-loss-every-day.html.
5. A Glossary of Archival and Records Terminology. The Society of American Archivists, 2005.
6. What is an information asset? The National Archives. Retrieved from http://www.nationalarchives.gov.uk/documents/information-management/ information-assets-factsheet.pdf on 9th September 2017.
7. Identifying Information Assets and Business Requirements. The National Archives, 2017. Retrieved from http://www.nationalarchives.gov.uk/ documents/information-management/identify-information-assets.pdf.
8. Managing Digital Continuity. The National Archives, 2017. Retrieved from http://www.nationalarchives.gov.uk/documents/information-management/ managing-digital-continuity.pdf on 11th September 2017.
9. DROID, the free file Profiling tool. The National Archives. Retrieved from http://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/digital-continuity/file-Profiling-tool-droid/.

Scanned with CamScanner