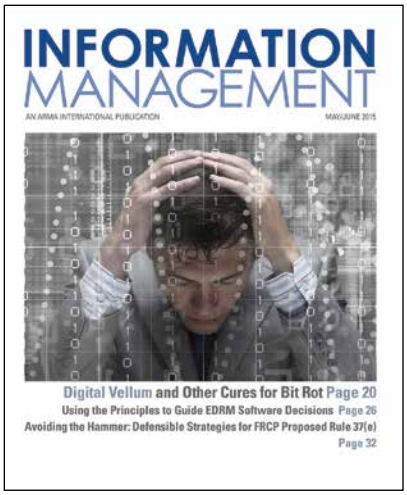
Protecting Organizations – and Culture – Through Digital Preservation



The decades-old challenge of digital preservation continues to be a major concern for information professionals, including several authors who contributed to this issue of *Information Management*.

Bit rot, which cover article author Marc Kosciejew, Ph.D., defines as "The irrevocable degradation or loss of digital information when the infrastructure (the hardware and software) required to access, interpret, view, and use this information is no longer available or executable," threatens every organization's ability to do business. Having grown in nature, size, and scope – and metastasizing at an accelerating rate, Kosciejew writes, bit rot also has the potential to wipe out contemporary (and future) history. His article explores the major causes for bit rot and its most promising solutions.

The importance of information to cultural preservation is the main theme of a case study written by Nancy Dupre Barnes, Ph.D., CRM, CA, about the United Nations Educational, Scientific, and Cultural Organization (UNESCO) World Heritage program.

According to Dupre Barnes, UNESCO's inter-continental efforts to retain cultural heritage is effected through proper information governance (IG); applications to be designated as World Heritage cultural sites require extensive documentation, including such records as ships' logs, religious relics, structural blueprints, archival photographs, census reports, and city planning maps. "IG provides the framework that protects those embedded assets," Dupre Barnes writes.

Preservation of electronically stored information (ESI) is the focus of the Katherine Aversano, J.D., and Joe Starnes, J.D., article about defensible strategies to comply with the Federal Rules of Civil Procedure's proposed rule 37(e) that could go into effect in December. Using these strategies will not only help organizations be prepared for e-discovery and avoid adverse actions a court might take if they are not, but also can help them satisfy public disclosure requirements and access their historical records.

The ability to place a legal hold to preserve ESI can be enhanced through implementing electronic document and records management (EDRM) software. Julie Gable, CRM, CDIA, FAI, writes about how organizations can use the Generally Accepted Recordkeeping Principles® (Principles) as a framework for evaluating EDRM applications – including the legal hold capabilities that are key for compliance with the Principle of Disposition.

"An important thing to look for is how the software product places a legal hold," Gable writes. "Must this be done one record at a time? Can an entire class of records be put on hold easily? Once applied, is there an effective way to communicate holds...? The software should maintain records of what has been destroyed and, of course, be able to destroy completely and irreversibly."

Gable also writes about how to use the Principles to determine the functionality EDRM software needs to help ensure compliance with the Principles of Integrity, Availability, Protection, and Retention.

For a primer on the closely related topic of implementing enterprise content management (ECM) software to tame the information explosion, see the RIM Fundamentals article by Shiva Hullavarad, Ph.D.; Russell O'Hare, Ed.D., CRM; and Ashok Roy, Ph.D., CBA, CIA.

Please let us know what other information would help you protect your organization; e-mail us at *editor@armaintl.org*.

Vicki Wiler
Editor in Chief