Is Your Electronic Stored Information (ESI) System Trustworthy?

By Virginia Jo Dunlap, Esq.

and

Robert Blatt, MIT, LIT

DATE

Contact:
Blatt@eid-inc.com
(805) 529 - 0600
www.eid-inc.com

Contact:
Dunlap@eid-inc.com
(916) 838 - 6917
www.eid-inc.com

EID
Electronic Image Designers, Inc.
Specializing in Electronic Content Management Technologies

Of course the document management system that your company has developed over the years is trustworthy -- or is it? You've invested in security to make sure that it is safe from hackers; your back up systems make sure no data is lost. Therefore, seemingly your system is "trustworthy".

But not so fast. Before you reach that conclusion you might want to check the AIIM best practices found in the June 15, 2009 updated release of ARP-1 to be sure. ARP-1 (2009) provides the parameters for helping you determine whether your document management system (also referred to as a content management system) meets the best practices of the industry for a "trusted system." Similar guidelines are expected from the international community later this year, as ISO reissues Technical Report 15801.

Lawyers and judges are beginning to awake to the issue that if evidence is stored electronically it may not necessarily be reliable. And, if it is not reliable, it may not be admissible at all (failure to lay a proper foundation including authenticity)[1] or it may be left to the trier of fact to decide how much weight to give the electronic evidence in the face of other evidence. Maintaining electronically stored information (ESI) in a trusted system or environment that meets the best practices as recently identified in ARP-1 (2009) will provide a methodology for showing the factual specificity necessary to for a witness to lay the proper foundational basis for electronic evidence.

ARP-1 (2009) provides keys to developing a trusted ESI system

As Section 5.3.3. of ARP-1 (2009) states, a document management system must have several key components in order to be considered a trusted system. Security and multiple copies are two pieces of the puzzle, but so is having a combination of media, hardware and software that prevents unauthorized alterations, an ability to independently verify the storage processes through audits, and policies and procedures to support the system. It does little good to have designed the best storage system in the world and then fail to tell anyone how to use it properly.

> ***A trusted document management system ensures that that all electronically stored information can be considered to be a true and accurate copy of the original information received regardless of original format.***
>
> ~ ARP-1 (2009) §5.3.3

Security and location of the ESI

In addition to prohibiting access from outside the organization, consideration must have been given to who has access to the ESI from within the organization and where and how it is stored.

To meet the best practices, as identified in section 5.3.1 of ARP-1 (2009), a trusted system must generate two separate copies of ESI when it is created. And, that "[t]he trusted document management system must write at least one copy of the electronic document or record into electronic media that does not permit additions, deletions, or changes to the original document and that is to be stored and maintained in a safe and separate location."

For example, it would not be within industry best practices to have a system that when a hard copy document is scanned it generates only one copy that is later backed up through the disaster recovery protocol. Industry experts believe that by generating multiple copies to separate locations at the time the document is created substantially reduces the risk of failure, loss, or alteration of the original document so as to better protect the integrity of the information stored.

Integrity of the information

By requiring the storage of information in a system that uses hardware and media methodologies to prevent "additions, modifications, or deletion" ARP-1 (2009) has captured the concept that users must have confidence in the accuracy of the stored information. A document management system that does not provide the users with confidence that the information put into the system may be regenerated accurately is of diminished or no value. In fact, it may end up with a negative value if it requires additional costs to provide that needed assurance to accuracy.

For example, in the context of producing records for a litigation request, someone in the entity must be able to verify that the documents generated were "true and accurate" copies of the documents maintained. Absent the level of confidence generated by following industry best practices, companies will have an uphill battle demonstrating their documents are accurate, unless they also maintained the original documents from which the ESI copy was produced is compared. This would result in inefficiencies in the business including increased costs in storage and time to review and compare the documents.

The standard setting committee that developed ARP-1 (2009) left latitude to designers to create a system utilizing hardware, software and media that best meets the needs the particular business organization. For example, an entity that modifies its original document throughout the course of the document lifecycle by appending information may have an entirely different design to its system than an entity that simply needs to maintain the original information. Regardless of how each system is crafted, it must consider preserving the integrity from the original source.

Audit trails & Historical Data

Another important aspect to the overall document management system is having an independently verifiable audit trail that can demonstrate the ESI has not been altered inappropriately. Once again, this provides added confidence to the end user that the documents maintained and/or generated from the system are accurate. The level of information that is available within document management systems can be at the level of who opened and printed, to who took what actions including workflow notations and/or routing to other users for review/processing. Being able to demonstrate reliability is directly related to both security AND appropriate levels of all forms of historical data that comprise the various audit trails.

Policies and Procedures

The final component identified as a best practice in a trusted document management system is the creation of and use of policies and procedures to support the system. It does little good for a document management system to be created if there are no guidelines for the type of information to be stored or identifying what methodology will be used to generate ESI.

For example, a business that transacts with clients via email should consider a policy for when an email should be stored in the document management system, giving guidelines for how employees should know whether it should be stored and how to implement the policies. Absent those types of policies, employees will have little guidance and differing practices for when email communications are stored in the system will develop throughout the organization.

Conclusion

Overall, ARP-1 (2009) has sought to provide some broad parameters identifying the industry best practices when it comes to determining the trustworthiness of the document management system. Meeting these industry standards will go a long way to generating confidence in the storage of ESI and eliminate litigation over the simple question of whether the document is a true and accurate rendition of the original.

[1] *In re: Vee Vinhnee* 336 B.R. 437 (B.A.P. 9th Cir. 2005) where evidence was excluded because the creditor (American Express) could not lay a proper foundation for the electronic evidence of the debt allegedly owed. *See also Lorraine v. Markel American Insurance Co.* 241 F.R.D. 534 (D. MD 2007) cross motions for summary judgment were denied for failure to address evidentiary issues with electronic evidence.

Virginia Jo Dunlap is a former securities regulator and litigator who developed processes along with Mr. Blatt to allow for review and analysis of large volumes of ESI in large-scale investigations and cases. In the private sector, she has served as a general counsel for a non-profit and as a senior executive in charge of risk assessment and mitigation for a global company, including finding practical solutions to ESI issues.

Robert Blatt has more than two decades of experience helping clients with content management and workflow issues through the analysis, design and implementation of ECM systems. He is a recognized national and international subject matter expert in the ECM industry and is chairman of numerous national and international standards setting committees.