Electronically Stored Information and Cyberforensics

By Albert J. Marcella Jr., Ph.D., CISA

A New Age of Discovery

The US Sarbanes-Oxley Act, US Health Insurance Portability and Accountability Act, US Gramm-Leach-Bliley Act, Basel II, and the International Organization for Standardization's ISO 17799 and ISO 27000—has it been a struggle to comply with these guidelines and implement internal control standards? Well, it is not getting any easier.

While the noncompete, nondisclosure, acceptable-use and rights management policies had seemed difficult to articulate and then implement, those may soon seem like the halcyon days. The next set of policies is expected to be even tougher to define and implement. In addition, failure to do so will no longer be looked at as an outstanding noncompliance item in an audit report.

In the US, the world of records retention and content management, as most industry professionals knew it, was retooled on 1 December 2006, with the official enactment of the new amendments to the US court system's Federal Rules of Civil Procedure (FRCP). Those rules now require any business that may find itself involved in litigation in US federal court to retain and manage electronic records.

The term "electronically stored information" (ESI) is applied to today's vast array of electronically generated documents, encompassing more than storage and retention, while ensuring that ESI generated by an enterprise is secure and protected from unauthorized access, use or destruction.

Federal Rules of Civil Procedure

Electronic discovery in legal matters is a complex issue that cannot be ignored. Consider the massive volume of enterprise data located in file systems, applications, preprimary storage and archives, and then recognize that it may be, at any time, discoverable. The new US rulesmerely underline what was already known: as ESI has become the norm, these records must be made available in the course of litigation. These new rules make this mandatory and require organizational discovery processesto be redesigned.

The new rules require that company attorneys and IT managers be able to demonstrate how ESI is stored; the procedures established to manage, control, protect and retrieve them under court order; and the policies governing their retention. In addition, the new rules require evidence of an established history and implemented routine for the deletion of corporate ESI. Feigned ignorance and plausible denial are matters that may have satisfied judicial inquiry in the past, but they are no longer tolerated by US courts. Noncompliance risks the most serious of consequences. In 2005, the Alabama (USA) Circuit Court of Appeals fined General Motors US $700,000 for delaying a discovery process by 98 days.

Legal Impact

Surveys completed by several organizations clearly show that a large percentage of corporations are either unaware of this new federal ruling and its impact on their day-to-day operations or, if they are aware, they are underprepared to comply should they be compelled to do so. For example:

- In a Cohasset Associates survey, nearly 50 percent of respondent organizations have no e-mail retention policy in place.[1]
- The ability to handle difficult e-discovery matters is a source of concern for most enterprises surveyed by law firm Fulbright & Jaworski. Just 19 percent of respondents consider their companies to be "well prepared" for e-discovery issues, while the vast majority (81 percent) report being "not at all" to "somewhat" prepared. More than a third of the UK contingent (35 percent) feel "not at all" or "poorly" prepared, while 23 percent of the US respondents fall into this category. Even the largest companies demonstrate little confidence in their preparedness, with just 19 percent feeling well prepared. No one reported feeling completely prepared.[2]

ESI As Evidence

A significant difference exists between the US criminal and civil court systems. The chief difference is that in a civil case, the victim controls essential decisions shaping the case. It is the victim who decides whether to sue, accept a settlement offer or go to trial.

In the civil justice system, liability must be proven by a preponderance of the evidence, which simply means that one side's evidence is more persuasive than the other's. In other words, the plaintiff must prove there is a 51 percent or greater chance that the defendant committed all the elements of the particular wrong. This standard is far lower than the "proof beyond a reasonable doubt" required for a conviction in the US criminal justice system.

It may not be a case of "if" but more realistically "when" this fact will compel enterprises to take a hard look at their ability to identify, retrieve and produce requisite ESI.

An enterprise must ask itself or, better yet, ask its senior management what the likelihood is that it will face the need to produce ESI and whether the enterprise is prepared to respond within mandated time frames.

Additional findings from the Fulbright & Jaworski survey indicate that large companies (more than US $1 billion in annual revenue) face an average of 556 lawsuits worldwide and spend an average of US $34 million on legal costs. The survey of 422 members of in-house counsels also found that 89 percent of respondents reported at least one new suit filed against their company in the past year.[3]

Today's reality is that "93 percent of all business documents are created electronically."[4] When coupled with the decreasing cost of storage, this allows "[t]oday's 'digital packrat' [to] hoard astronomical quantities of electronic information. …According to a recent article in the *Wall Street Journal*, 'We went through a belief that storage was cheap so we could save everything'…[and] although storage may be cheap or free,…it is not necessarily the wisest decision for an organization to make."[5]

Laura Bandrowsky, chief operating officer of Wescott Technology Services LLC, cautions, "The volume of data that must be managed or handled for litigation directly affects the cost of discovery."[6]

In the eventuality of e-discovery, cost containment is the challenge.

Hold Management and Spoliation

Two important concepts related to ESI are hold management and spoliation.

Hold management refers to the ability to respond to a legal action. Once an enterprise is notified of a legal action, all records that may relate to that action are placed on legal hold. They may not be destroyed and their profile information may not be modified. They must be prevented from destruction until the hold is lifted. The ability to hold records may also be applied to audit situations when required.[7]

Loss or destruction of evidence exposes litigants to drastic monetary, evidentiary, criminal and other sanctions, including, in some jurisdictions, liability for the tort of spoliation.[8]

Spoliation of evidence refers to the willful destruction of evidence that is germane to the case in litigation. This would include destruction of ESI. However, given the volume of electronic documents created in virtually every business today, it is usually necessary to delete, archive and/or overwrite documents in the routine and normal course of business. Accordingly, many companies have data management systems and/or data retention policies in place, which include deletion of ESI on a regular basis.

Spoliators of evidence in legal actions are individuals who neglect to produce evidence that is in their possession or control. In such a situation, any inferences that might be drawn against the party are permitted, and the withholding of evidence is attributed to the party's presumed knowledge that it would have served to operate against him/her.[9]

Safe Harbor

Section 26(f) of the FRCP provides for a safe harbor against sanctions being imposed in the event of electronic information that might be lost under the "routine, good faith operation" of such a data management system or data retention policy. It is important to remember, however, that this amendment does not provide a shield for any party "that intentionally destroys specific information due to its relationship to litigation or for a party that allows such information to be destroyed in order to make it unavailable in discovery by exploiting the routine operation of an information system."[10]

Figure 1 summarizes the expected impact of the new amendments on an enterprise's IT policies and procedures. The auditor is advised to assess these changes with respect to the impact that they may have on the auditor's internal IT practices and policies.

Figure 1—Impact of New US Amendments

Amendment	Effect on IT
Rule 16(b): A description of all electronically stored information must be presented within 99 days of the beginning of a legal case.	E-mail archiving, retention software and policies should be put in place.
Rule 26(a): Electronically stored information, including e-mail, must be searched without waiting for a discovery request.	E-mail archiving and retention policies should be put in place by IT so information can be discovered rapidly.
Rule 26(b): A party need not provide discovery of electronically stored information if there is an undue burden or cost.	The enterprise is required to prove that installation of e-mail archiving software is an onerous expense.
Rule 26(f): Litigants are required to discuss any issues relating to preserving discoverable information.	Legal counsel is required to know how e-mails are being retained and how they can be searched and retrieved.
Rule 34(b): The requesting party is required to designate the form in which it wants ESI to be produced; the responding party is required to identify the form in which records will be produced.	IT must be aware of how e-mails are stored, e.g., on disk or tape, and how they will be retrieved.
Rule 37: A safe harbor provision for deleting records must be established.	IT may establish policies for the deletion of e-mail.

Moving Forward With ESI

Given the volume and variety of communications that pass through an enterprise on any given day, the absolute necessity for a viable, well-thought-out, well-planned and well-tested document management program is essential to the survival of the 21st century corporation. Add to that the legislatively mandated requirement that any business that may find itself involved in litigation in US federal court must have procedures in place to retain and manage electronic records, and the motivation for a document management program goes from a need to a business requirement.

Identifying exactly which corporate communications must be retained and then establishing the appropriate procedures to do so takes time, energy, effort and financial resources. Assessment by the enterprise's internal audit function or review by an external third party must be built into the overall program to ensure compliance and corporate readiness.

Weaknesses in the enterprise's document management program must be corrected, and appropriate controls that endeavor to maintain a compliant document management program and provide management with the information resources necessary to respond effectively, appropriately and in a timely manner to a court order requiring the enterprise to produce ESI must be implemented.

Global Perspective

While the FRCP and its application to ESI, as noted previously, is US-centric in its application, these principles, along with the recommendations presented for implementing vigilant internal controls, are truly global in their implication and application. Enterprises that may never anticipate stepping foot into a US federal court can benefit greatly from an assessment of their current document management procedures and subsequent implementation of a well-designed strategy to control organizational ESI. They benefit by achieving an overall better-controlled records management and retention process, having an ability to identify critical ESI, establishing retention and destruction cycles and access rights, and ultimately being better prepared to meet the potential for similar emerging legislation in their own countries.

Auditing ESI Preparedness

As regulators and courts increasingly recognize the enhanced and richer information value of electronic data compared with physical documents, companies should strengthen their ability to safeguard their rights and respond appropriately.[11]

The points, actions and activities provided in the sidebar, "ESI Audit Considerations," should be examined as potential recommendations to management. These practices may be implemented to establish an enterprisewide, proactive document management program that addresses the issues of compliance and governance, assists in mitigating potential legal culpability, and establishes solid internal controls for corporate ESI.

ESI Audit Considerations

1. Have a plan and a process for discovery of ESI that can improve over time.
2. Understand the end-to-end process from discovery to production and the implementation of "holds." This encompasses methods and practices that make sense for the enterprise, understanding where technology is needed to facilitate or improve process efficiencies or quality of results, and identifying the specific technology capabilities that are required to make the end-to-end process effective. It is best accomplished through a cooperative effort among legal, IT and the line-of-business (LOB) organizations.
3. Consider technology capabilities such as dedicated computer storage and processing resources with robust security, inventory and identification of ESI sources potentially relevant to the request.
4. Examine search and retrieval tools that can be responsive to the request and are robust enough to deliver results in tight time frames, with the appropriate degree of precision.
5. Consider integrated content management, which provides "middleware" to link multiple sources of ESI for search, retrieval and possible collection, if there are multiple content sources.
6. Conduct benchmarks to test and establish parameters for various electronic discovery scenarios. Repeatable processes that have been tested to provide evidence of results of sought-after records production for a given set of metrics can be a significant key to negotiating e-discovery requests. This will help effectively plan the response activities and time frame and prudently apply resources and budget.
7. Develop repeatable processes that have the flexibility to accommodate a variety of discovery and regulatory requests.
8. Develop and implement records management and retention policies that can effectively preclude retaining nonmaterial information. Formal guidance to promote the appropriate and prompt disposal of unneeded ESI is an important component of records management.
9. Maintain an inventory of ESI sources that documents system descriptions and characterizations, such as computing system and location, software product and version, business purpose and scope, data storage (active drives or archives), retention location and periods for backup data, estimated volume of data being retained, and native capabilities for search and data formats. This inventory provides auditors and legal counsel with the data needed to estimate electronic discovery time and costs and determine an efficient and reasonable approach to develop the body of material for legal review.
10. Implement an ESI records management program that controls the volume of information through appropriate and regular destruction of ESI in the normal course of business.
11. In addition to establishing and implementing destruction policies through the records management program, provide the mechanisms and protocols to suspend destruction for the specific ESI required to comply with discovery and preservation orders.
12. Keep pace with changing regulations, new requirements and trends in enforcement.
13. Have a process whereby compliance or regulatory affairs, or whatever entity has the responsibility to monitor regulatory initiatives and implement compliance measures for new regulations, communicates the requirements across the enterprise. These communications include, for example, legal, technologies, risk management, records management, audit and relevant LOB management.
14. Reach an understanding of the potential impact of legislation such as Sarbanes-Oxley and Basel II (financial services) on requirements for controls and audit trails across intraorganizational boundaries.
15. Review and appropriately update, in a timely manner, records management mechanisms, technologies and protocols for retention and destruction.
16. To avoid increasing risk and costs of noncompliance, do not just update the records retention and management program, but completely overhaul it. This requires knowledge of electronic records, records management,

ESI technology issues and characteristics, and the total information fabric of the business that encompasses information in all forms.

17. Create an effective records management program for ESI. This considerably reduces volumes of physical material held in storage and significantly decreases discovery efforts and production of physical records.
18. Effectively use electronic discovery and search tools, and establish a consistent team with appropriate skills in electronic discovery and knowledge of the company's ESI sources, technology platforms and tools.
19. Establish a set of tools that can provide predictable results based on established protocols.
20. Periodically conduct benchmarking exercises against a variety of ESI sources to establish metrics using the enterprise's tools of choice. These metrics help to establish the time frames and costs of searching various electronic source systems using various scenarios and parameters. For example, how long does it take to search and report results on 20 named individuals in the enterprise's e-mail system regarding one matter over a period of three years?
21. Understand the metrics and time requirements for simple search, de-duping and creation of "collection" stage files, separate from the time and effort required for legal or other reviews, advanced searching, and culling of irrelevant or privileged information. Conduct the benchmarking on current systems, retired systems and archive systems.
22. Implement hold management rules (prelitigation identification of potentially material information and ongoing implementation of document preservation orders) that require special attention and tools for ESI. The rules that will determine which ESI are to be held (beyond their scheduled retention period) require careful crafting (by legal counsel, perhaps with assistance from IT and LOB managers) and an analysis of holdings in the context of ESI and business systems. A lack of a clearly defined "registry" for records (such as what can be provided by a document management or records management system) to which the rules can then be applied constrains adoption of automated techniques and can lead to an outcome that all ESI is "on hold forever."
23. Consider the information fabric of the enterprise and create policy-based rules for managing ESI that not only facilitate discovery and document production activities, but yield business benefits as well. Defining and incorporating records life-cycle-based controls and retrieval protocols also facilitate meeting trustworthiness and authenticity requirements.
24. Make retention decisions in the context of what the data represent, where they reside, longevity of preservation and vitality of systems.
25. Evaluate systems (sources of ESI) and determine how older information might be accessed reasonably. If it cannot be accessed reasonably, critically examine why it is being retained.
26. Implement policies and records-destruction practices in accordance with documented protocols that become part of the normal course of business.
27. Update IT governance practices to include identification of retention requirements (based on legal, regulatory or other factors) in the design requirements for new systems.
28. Consider the impact of encryption policies on search and retrieval capabilities. With the increasing adoption of encryption for e-mail and attachments, there are concerns that e-mail will not be searchable because of "loss" of the appropriate encryption keys, introducing further complexity to maintain accessibility of aging ESI. ESI that is subject to production, but cannot be decrypted, could result in raising suspicions of spoliation.
29. Consider the impact of destruction methods and available technology.
30. Multiple regulatory requirements can pertain to any particular class of ESI. Therefore, when there are changes in any particular regulation affecting records, evaluate the impact of that change on the retention policy in consideration of other requirements that might apply.
31. Establish standard practices (automated where feasible) for regular destruction of ESI (e.g., on a monthly or quarterly basis) that are not unduly burdensome on employees. Establish communications and oversight practices that reinforce awareness and promote compliance. Destroy ESI as soon as possible, on a regular and consistent basis, and use methods that promote security and privacy for the information being destroyed.
32. Because many retention periods are triggered by an event, determine an event notification to the records management system to trigger the start of a defined retention time period. Any ESI that is on hold would have the retention period trigger set "on" when the event has occurred, but would not be destroyed until two conditions are met: the "hold" was lifted and the retention period has expired.
33. Establish basic metadata to be maintained as part of the record for each class of ESI, and implement metadata standards.
34. Identify audit trail requirements when developing metadata standards. If there are requirements for traceability and chain of custody, e.g., capturing (as metadata) who did what and when they did it, make them part of the metadata standard.
35. Ensure that the legal team is armed with an understanding of what ESI is or what is not accessible before entering electronic discovery negotiations.

Endnotes

[1] Connor, D.; "New E-Records Rules: Who's Complying?," *Network World*, vol. 23, iss. 47, 4 December 2006, p. 16

[2] Fulbright & Jaworski, "Third Annual Litigation Trends Survey Findings," USA, *www.fullbright.com*, October 2006

[3] *Ibid*.

[4] Lange, M. C. S.; "E is for Evidence: Using an Online Repository to Review and Produce Electronic Data," *Journal of Internet Law*, vol. 6, iss. 12, p. 18-21, June 2003

[5] Myler, Ellie; "The ABC's of Records Retention Schedule Development," *E-DOL*, May-June 2006

[6] Garretson, R.; "A Lifecycle of Its Own," *CIO Insight*, iss. 76, December, 2006, p. 81-89

[7] *www.cmswatch.com/GlossaryTerm/137*

[8] Collins, C.; "California Eliminates Intentional Spoliation Tort," Thelen Reid & Priest LLP, 21 July 1999, *www.thelenreid.com/index.cfm?section=articles&function=ViewArticle&articleID=1088*

[9] The Gale Group Inc., *West's Encyclopedia of American Law*, "Spoliation," 1998, *www.answers.com/topic/spoliation*

[10] Cortese Jr., A. W.; "Proposed Amendments to the Federal Civil Rules Strike a Healthy Balance," *Defense Counsel Journal*, vol. 72, iss. 4, October 2005, p. 354-361

[11] Churchill, B., et al.; "The Impact of Electronically Stored Information on Corporate Legal and Compliance Management: An IBM Point of View," IBM Corp., USA, October 2006 (used with permission), *www-03.ibm.com/industries/financialservices/doc/content/bin/fss_the_impact_of_eletronically.pdf*

Author's Note

This article is based on the author's recent book *Cyber Forensics II: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2nd Edition*, and excerpts are reprinted with permission of the publisher Taylor & Francis Group.

Albert J. Marcella Jr., Ph.D., CISA
is president of Business Automation Consultants LLC, a global IT and management consulting firm. Marcella is an internationally recognized public speaker, researcher, and workshop and seminar leader with 30 years of experience in IT audit, security and assessing internal controls. He is the author of numerous articles and 28 books on various IT-, audit- and security-related subjects.

Information Systems Control Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *Information Systems Control Journal*.