# ELECTRONIC RECORDS CREATE DIFFERENT RISKS

In a modern economy dependent upon automated processes, using electronically stored information creates speed and efficiency. At the same time, the dependence on ESI may result in liability risks for unwary businesses. Indeed, a paperless workplace may inundate even the brightest executive with mounds of information that is everywhere and nowhere at the same time. Effective electronic-records management will allow businesses to retrieve information efficiently, helping them compete successfully in a global marketplace.

ESI includes any information or process that can be stored or read in a digital format: e-mail, word-processing files, Web pages, spread sheets, documents scanned and stored in various formats, audio files and photographs and other digital images. Such electronic information is different from its paper counterpart. First, electronic documents are created at a much faster pace. Second, electronic documents are harder to dispose of than paper documents, in that the deletion of a file from a desktop does not remove it from the computer's storage devices. Third, unlike paper documents, computer information is dynamic and can be changed without human intervention, such as with an application

**Companies should take steps to manage ESI for legal, compliance and litigation purposes.**

that is designed to update files from another location automatically. Finally, electronic data is dependent upon its software or database environment to be used effectively, which can be problematic when technology changes require the movement of data from one program to another while upgrades are taking place.

For most businesses and executives, ESI and its related technology require a constant learning process. While most of us have come to understand concepts such as desktops, laptops, PDAs, CPUs, hard drives, memory and encryption, the world of e-commerce in business and e-discovery in litigation requires a speaking acquaintance with terms like ghost image, forensic or mirror image, allocated and unallocated space, hash value, metadata, legacy data, orphan records, WORM media and life-cycle management. With ESI usually accessible and searchable, businesses have developed a false sense of security about their ability to safeguard and manage business capital created on a daily basis.

In most cases, businesses have navigated, albeit awkwardly, the various record-retention requirements in areas involving the Internal Revenue Service, the Occupational Safety and Health Administration, the Health Insurance Portability and Accountability Act, pharmaceutical research, health care and financial services. Each regulatory body has its own retention period, which in many instances has resulted in a "keep everything forever" approach. With the correct indices and search tools, most businesses have created, stored, and transferred transactional information and communications with relative ease. To ease the burden of storage, IT professionals have created automatic archival and deletion protocols that, in large measure, are consistent with business and regulatory objectives.

The ability to create and store electronic data has resulted in increasing demands by third parties to preserve, retrieve and produce ESI in legal, compliance and litigation contexts. These burdens are exacerbated by seemingly innocent archival and deletion protocols, which have sometimes contributed to a "perfect storm" of lost data, lack of accountability and, in extreme cases, enormous legal risk and financial liability. The evolution of "e-discovery" in government investigation and civil-litigation proceedings has exposed flagrant

lapses in electronic-records management and e-discovery programs. In a recent case involving the failure to search the company computers of certain employee witnesses for relevant e-mail communications, a federal court levied a fine of more than $8 million against the offending litigant. There are hundreds of reported decisions where state and federal courts have considered issues relating to the discovery of electronic information.

Recent amendments to the Federal Rules of Civil Procedure require litigants to meet and confer early in the litigation process to identify and preserve ESI that may be the subject of subsequent discovery. Many jurisdictions, including Arizona, Arkansas, Illinois, Indiana, Maryland, Utah and the Business Court of North Carolina, have followed suit. These rules also provide for a joint effort to use common and searchable formats for production and mutually agreeable search terms for forensic study of the adversary's records. In addition, state and federal agencies such as the U.S. Department of Justice and many states' attorneys general routinely seek early dialogue with companies subject to subpoena or investigation so as to avoid the inadvertent loss of relevant data. Finally, the federal courts have adopted a "safe harbor" rule to forestall the imposition of sanctions for a loss of ESI as a result of the routine, good-faith operation of an electronic information system. Examples include the failure to retain obsolete software that might be needed to access ESI stored in older applications, inadvertent reactivation of overwriting protocols for backup tapes, and the exclusion, in the review process, of personal storage devices maintained by individual employees, unbeknownst to company counsel or IT personnel.

In anticipation of these demands, and to avoid the organizational and financial risks demonstrated above, companies should take steps to manage ESI for legal, compliance, and litigation purposes. These include:

- Review of e-mail management policies to reduce storage of older documents.
- Use of newer technologies, such as content-integration applications, to design and implement ESI storage protocols across the business enterprise.
- Adoption of an electronic-record-retention plan that is in accordance with the requirements of applicable regulatory authorities.
- Establishment of formal protocols to suspend the destruction of ESI in the event of an investigatory or litigation event.
- Use of periodic audits by legal and IT personnel to test systems and ensure ongoing compliance.

## Robin K. Vinson

Robin Vinson is a partner in the Raleigh law firm of Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan LLP, practicing in the areas of corporate, contract and regulatory law and complex corporate, contract and tort litigation. He earned his bachelor's and law degrees from Wake Forest University. He has written and spoken on corporate-compliance, record-retention and risk-management issues for public and closely held companies.

- Prohibitions on the use of personal e-mail accounts and home personal computers to conduct company business.
- Establishment of procedures to maintain the chain of custody of ESI when retrieved for a government-agency investigation or civil litigation.
- Preservation and security of intellectual property, proprietary information, trade secrets and other confidential business information.

These steps are vital for the organizational and economic success of companies doing business in the digital age. Fortunately, an overwhelming majority of American businesses are addressing ESI compliance issues on an enterprise-wide basis, and many are using content-integration technology to move toward common technical platforms. Examples include the use of application-programming interfaces and policy-based archive systems to preserve e-mail. As businesses progress toward competence in their management and procedures in these areas, there will be an increasing demand for IT personnel who have corporate and forensic expertise. Likewise, companies should expect and demand that their legal counsel be well-versed in the technical jargon of ESI, record-retention periods applicable to their businesses and their requirements and uses in legal, compliance and litigation matters.