



Managing Corporate Evidence: Empowering Defendants and Respondents

*Rob Peglar
Vice President, Technology, Marketing
XioTech Corporation*

November 2006



IMPORTANT NOTICE

By accepting, reviewing, or using this document, you, as the recipient, agree to be bound by the terms of this notice. Information in this document is subject to change without notice. Names and data used in examples are fictitious unless otherwise noted. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred. Xiotech and/or its licensors may have patents or pending patent applications, trademarks, copyrights, or other intellectual property rights covering the subject matter in this document.

The configuration(s) tested or described in this document may not be the only available solution(s). This document is not intended (nor may it be construed) as an endorsement of any product(s) tested, as a determination of product quality or correctness, or as assurance of compliance with any legal, regulatory, or other requirements.

This document provides no warranty of any kind, including, but not limited to, any express, statutory, or implied warranties, whether this document is considered alone or in addition to any product warranty (limited warranties for Xiotech products are stated in separate documentation accompanying or relating to each product). No direct or indirect damages or any remedy of any kind shall be recoverable by the recipient or any third party for any claim or loss in any way arising or alleged to arise from or as a result of this document, whether considered alone or in addition to any other claim.

Xiotech, Magnitude 3D, Magnitude, REDI, Dimensional Storage Cluster, SAN in a BOX, TimeScale, DataScale, GeoRAID, and Zero Server Footprint are trademarks or registered trademarks of Xiotech. All other trademarks or service marks are the property of their respective owners. The reproduction of any trademark or service mark, registered or otherwise, belonging to any third party appears in this document for the purposes of identification of the goods or services of that third party only. No license of any kind is provided by Xiotech and/or its licensors to any party because of this document. No right or title in any mark or other proprietary interest is transferred by Xiotech and/or its licensors to any party because of this document.

The Intelligent Control (ICON) management platform employs an Intel® processor.

© 2005, 2006 Xiotech Corporation. All rights reserved. P/N 070402-1106.



6455 Flying Cloud Drive
Eden Prairie, MN 55344-3305
phone: 1.866.472.6764
www.xiootech.com

Table of Contents

The Nature of Electronic Evidence	1
Evidentiary Issues and Integrity of Evidence	2
Corporate Evidence Management – Taking Back the Power	3
Conclusion	5

Dramatic increases in civil and criminal litigation, and the increasingly sophisticated use by attorneys of electronic evidence discovery (EED) has rendered traditional methods of corporate information management unacceptable to the modern corporation. From a litigation risk management (LRM) perspective, most corporations are ill prepared either to respond to discovery motions and inspection orders, or to mount informed and effective defensive strategies because they do not consider the electronic evidence within their organizations—millions of documents, spreadsheets, presentations, electronic mail, and instant messages, and all their copies, versions, archives, and backups—as potential evidence. Evidence that might be—and increasingly is—used against them.

Traditional methods of dealing with these masses of data—records and document management technologies—are entirely inadequate to meet the burden of discovery and proof now placed on a defending firm.

The Nature of Electronic Evidence

In written opinions... courts granted sanctions 65% of the time, with defendants being sanctioned four times (81%) as often as plaintiffs. The sanctioned behavior most often involved the non-production, i.e., destruction of electronic documents (84%), rather than a delay in production (16%). When parties were sanctioned for delay, the late production was sometimes coupled with some form of deception or misrepresentation to the court, such as the fabrication of evidence or falsely claiming that documents did not exist (43%).¹

Electronic evidence has fundamentally changed how corporations must manage and store their business records. To manage litigation risk and minimize overall litigation costs, corporate information—particularly the body of information we refer to when we use the word “document”—must be managed with the understanding that every document created and distributed inside the company today is, potentially, discoverable evidence.

Virtually every piece of data stored in the corporation must be managed in this light—from office applications to emails and instant messages, to financial working papers and even the seemingly benign data often found on corporate servers and desktops. The sheer volume of that (discoverable) evidence in the typical firm is staggering. In 1999, 90 percent of corporate information was stored in digital form, with millions of legally relevant transactions being conducted electronically every day.²

Electronic evidence, by its sheer volume and very nature of the medium, raises some complicated issues:

- **Electronic documents outlast paper documents**, yet they are often not under the control of corporate records and document management, if such management exists at all.
- **Electronic documents exist in many forms and in many places** and are, therefore, easier to find during discovery—and are much more complex for corporations to control.
- **Electronic documents carry data about themselves** that describes where they have traveled, who has seen them, and who has altered them—providing far more detailed evidence trails than paper documents.
- **Electronic documents often carry embedded data** that can reveal a wide array of pertinent, yet not obvious evidence—from commentary concerning the content itself to a complete history of all modifications made to the document in question.

The complexity introduced by electronic documents is further demonstrated by the evidentiary issues that have frustrated defense efforts in numerous highly publicized cases. As seen in recent cases, judgments or fines are often levied against corporations due to their assumed lack of evidentiary controls, both ahead of a suit and during discovery, following civil action.

The high-profile case *Perelman v. Morgan Stanley* demonstrates the severity of sanctions that can result from a corporation’s inability to produce evidence in a timely, comprehensive manner. The court

1. “Electronic Discovery Sanctions in the 21st Century”, Scheindlin & Wangkeo

2. A single 650MB CD-ROM can contain the equivalent of 5 boxes of—nearly 75,000 individual—paper documents.

entered a default judgment based on Morgan Stanley's "bad-faith" attempts to produce requested documents (they were unable or unwilling to produce archived emails in a timely fashion) and directed the jury that it must accept as fact that Morgan Stanley helped Sunbeam defraud investors. The jury awarded Mr. Perelman in excess of \$600M in compensatory damages and \$850M in punitive damages.

Evidentiary Issues and Integrity of Evidence

There are two primary areas where such evidentiary issues and the integrity of evidence most often impact a defense:

- Retention and destruction of evidence
- Sequestration of evidence

Retention and Destruction

Retention and destruction policies for electronic records are receiving significant attention in the courts today. Having a retention policy in place that is consistently enforced is critical for a successful defense. Many companies can show that policies are in place, but discovery often reveals that these policies were not consistently enforced—which is often more damaging than having no policy at all, and can result in a judgment against the corporation. Adjacent to retention and destruction is the risk of *spoliation*.

Simple negligence (e.g., accidental destruction of documents) is not an excuse and can lead to spoliation claims—which may result in summary judgments, fines, or seizure of corporate computing infrastructure assets. To avoid spoliation claims, corporations must define and enforce retention and destruction policies on a consistent and corporatewide basis. Further, corporations must be able to effectively protect evidence from intentional or accidental destruction, through comprehensive sequestration techniques.

Sequestration

Sequestration is the ability to quickly and effectively isolate specific electronic evidence for both corporate protection and court-ordered actions. Sequestration is applicable in actions ranging from hold orders to protection of privileged and generally available evidence.

- **Hold Orders:** When a Hold Order is issued, all evidence—including paper and electronic documents—must be preserved intact from that point forward. The accidental destruction of data (e.g., misplaced backup tapes) is not an acceptable cause of noncompliance with a Hold Order. The ability to comply with a Hold Order is critical to a successful defense, yet most of today's corporations would not have the means to successfully implement and enforce a Hold Order.
- **Protection of Privileged Evidence:** One of the common areas of concern for defense litigators is the immediate sequestration and continuous protection of any and all evidence and work product related to a potential or in-process suit. Often confidential work product or client/attorney privileged information is poorly handled, resulting in its admission by the courts as evidence.
- **Protection of Evidence in General:** Potential evidence is often accessible by employees and partners who may advertently or inadvertently disseminate it to the public. Efficient sequestration prevents such dissemination, retaining control of evidence by appropriate parties ahead of or during legal action.

The effective management of electronic evidence represents a new frontier for corporations. Yet today, most corporations are not taking the actions required to effectively and proactively manage electronic evidence to their best advantage.

Managing Litigation Risk - Taking Back the Power

The majority of organizations are not prepared to meet many of their current or future compliance and legal responsibilities. The majority of organizations are not doing what they need to do today regarding digital preservation to be prepared for the future. Certain asset management problems associated with electronic records have the potential to be devastating in terms of costs, professional careers, and even corporate reputations.³

To combat the effectiveness of EED tools, reduce legal costs, and improve their ability to proactively manage litigation risk, corporations need to continuously control corporate information as evidence—ahead of litigation. An effective evidence management strategy must be created and enforced across the corporation, dealing with all aspects of the capture, control, and ongoing assessment of all corporate evidence.

The transition to comprehensive effective evidence management, begins with a graded, step-by-step business process, similar in intent to Six Sigma process improvement programs (Fig. 1).

In implementing this stepwise process, corporations have the opportunity to:

- Prevent evidentiary issues that can result in negative judgments, thanks to comprehensive evidence controls.
- Move to be responsive in the case of a suit, quickly providing critical evidence to their defense litigators for development of defense strategy, while effectively responding to court production demands.
- Ultimately become proactive in their assessment and response to litigation risk in advance of any civil litigation.

An effective corporate evidence management business process starts with the realization that all electronic information in the corporation must be effectively managed in light of its potential use as evidence—both in favor of and against the corporation. Without this change in thinking—among general management, compliance, custodial, records management, and IT personnel—the organization will continue to face unknown and substantial litigation risk occasioned by unmanaged documents.

Accepting the *fundamental fact that all documents are potentially damaging evidence* leads companies immediately to *evaluate their current infrastructure and processes* for document capture, distribution, and storage. Most often, these companies find the needed infrastructure (file servers, desktop drives, email systems, voluminous data archives, and scattered pockets of document and records management) and processes (publish what you want, when you want) lacking. Based on the knowledge of their current situation, with all of its inherent opportunities and threats, corporations can now move forward with the deployment of an effective corporate evidence management system.

The effective deployment of a corporate evidence management business process begins the foundational steps of implementing policies and technologies that support the prerequisite, preventive, and responsive capabilities. The four steps listed below are critical to addressing the business process of evidence management.

Step 0: Capture of Electronic Evidence

An effective evidence management business process will provide the ability to proactively capture and control all electronic evidence and metadata, including documents, emails, instant messages, reports, *3. Electronic Records Management Survey, 2003. Cohasset Associates, Inc, in association with AIIM International and ARMA International.*

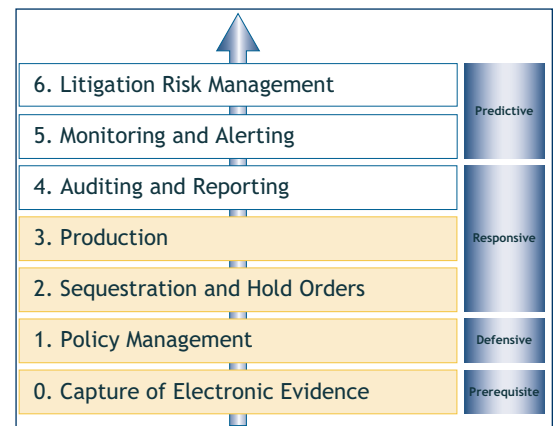


Fig. 1. Step-by-Step Evidence Management Process

working papers, and more—as it is created within the corporation. All captured evidence needs to be placed in a single, controlled evidence pool. Evidence is monitored and documented across its lifecycle from its creation, modification, transmission, and viewing to its ultimate retention and destruction. Both active and archived evidence needs to be placed under evidence control. Capture and control should be performed in a nondisruptive manner, ensuring the continued smooth operation of the business.

By capturing and controlling evidence in a proactive and continuous manner, corporations facilitate future discovery and production demands, reducing the overall cost of such discovery. The risks associated with current discovery practices that treat each discovery motion as a separate and discrete action are also minimized.

Step 1: Policy Management

All evidence within the pool is associated with specified retention policies, based on the classification/type of evidence and overall corporate and regulatory requirements. Retention and destruction of corporatewide evidence is enforced through the corporate evidence management system, with said enforcement audited for court admission. Ultimately, traditional, time-based backup approaches are replaced by continuous evidence-driven archiving and protection strategies that blend corporate operational needs and regulatory requirements with reduced-risk evidence management policies. With appropriate evidence retention and destruction policies working in conjunction with evidence controls, the “smoking guns” of unknown evidence found in today’s backup media are minimized as potential threats against the corporate defense.

Step 2: Sequestration and Hold Orders

As mentioned earlier, sequestration is the ability to quickly and effectively isolate specific electronic evidence for both corporate protection and court-ordered actions. Sequestration is applicable in actions ranging from hold orders to protection of privileged and generally available evidence. With a corporate evidence management system, legal counsel can confidently sequester information and execute a Hold Order.

Step 3: Production

The processing and production of electronic evidence involves the review, annotation, redaction, bates stamping, and physical output of data onto transportable media. Utilizing traditional processes, many organizations spend countless hours and are faced with large expenses in performing these tasks utilizing outside counsel or external consultants. With a well executed evidence management business process, organizations can take back the power and efficiently review and produce this evidence in house, significantly reducing both time and operating expenses.

Once an organization has addressed these basic business processes, the corporate evidence management system will allow them to focus on optimizing response and taking a proactive approach to managing litigation risk through the additional steps of auditing and reporting, monitoring and alerting, and litigation risk management.

An effective evidence management business process deployment will require a common vision and cooperation between executive management, counsel, and the IT professional staff. A phased approach can be taken toward such a deployment, focusing first on preventing common evidentiary issues, moving to a focus on effective and efficient production, and culminating in the ability to proactively define and enforce policies while aggressively assessing evidence for litigation exposure— ahead of any legal action.

Conclusion

Evidence management strategies promise to shift the balance of power toward defendants and away from plaintiffs by empowering corporations to more effectively and proactively manage and respond to ongoing litigation exposure.

Effective corporate evidence management promises to empower businesses by:

- Controlling all electronic documents as potential evidence for and against the corporation.
- Extending in-place infrastructures with the processes and policies necessary to ensure effective evidence management across the entire evidence lifecycle.
- Shifting the balance of power from the plaintiff to the defense by accelerating the development of defense strategy and tactical preparation.
- Making overall litigation costs more predictable, minimizing the costs of discovery, while eliminating costly corporate distraction and lost productivity.

In the age of electronic evidence, businesses must begin to deploy corporate evidence management strategies to proactively monitor, identify, and control litigation risk—as recorded in electronic evidence during day-to-day business operations. Technology can provide the mechanism for deploying an evidence management strategy as businesses begin to manage records as potential evidence. It is time to take advantage of these technology solutions and wrest litigation power from the plaintiffs—leveraging electronic evidence in favor of the corporation.