

# eDiscovery Challenges

**Tom Olzak**  
**February 2006**

During the past two decades, the shift from paper to electronic filing of business documents introduced a new challenge: meeting the requirements of litigation discovery. Not only are organizations keeping more information; the vast amounts of email messages and other types of documents are typically not organized in a way that facilitates quick, cost effective extraction from personal and enterprise storage.

If you're responsible for the security of your company's information, your role extends to protecting documents required by discovery requests. Are you prepared to assure your executive management, or to testify, that you've done everything reasonable and appropriate to meet the court's expectations?

In this paper, I explore the challenges of eDiscovery (Electronic Discovery) followed by recommendations that might help avoid the high costs of compliance – or non-compliance.

## The Challenges

According to Fulbright and Jaworski's Second Annual Litigation Trends Survey, electronic discovery is the top litigation issue (2005). Courts are getting tougher on companies that fail to provide documents, especially email, requested by Plaintiffs. The following are some examples of the results of non-compliance (Patzakis, 2006):

- Morgan Stanley suffered a default judgment of \$1.45 billion
- Phillip Morris incurred a judgment of \$10 million
- UBS incurred \$30 million

One of the problems associated with electronic discovery is the failure to locate documents and email because they've been deleted. But the routine deletion of documents is not a reasonable defense when faced with a discovery request. In the 2003 Zubulake vs. UBS Warburg case, the court found that the UBS attorneys failed to implement proper [litigation holds](#) to prevent the routine destruction of email. The following list describes the material points of the standard (CGOC, 2005):

1. Enable your "discovery liaison" to readily describe information custodians, systems, storage, and your retention policies
2. Affirmatively and repeatedly communicate legal holds to all affected parties
3. Integrate your retention policies and coordinators with discovery challenges and responsibilities
4. Actively manage and monitor document collections
5. Interview affected employees to determine sources of information
6. Monitor compliance with legal holds on an ongoing basis

7. Thoroughly document and demonstrate the efficacy of your process
8. Prepare to take responsibility for ensuring that information is preserved, collected, and produced.

The problems with electronic discovery are not always related to deleted documents. In many cases, documents exist on storage somewhere in the organization's data center. Locating it might be expensive or close to impossible. In these cases, management is faced with the decision to either incur the displeasure of the court or pay a consultant millions of dollars to scour the storage environment. Neither option is attractive to investors.

## **The Solution**

There are two basic types of documents with different archiving requirements – messages and electronic documents. For the purpose of this discussion, messages include email and instant messaging (IM) exchanges. Electronic documents include word processing and spreadsheet files.

Through the proper management of messages and electronic documents, companies can reduce the volume of information potentially subject to discovery and reduce the cost of collecting information (Roitblat, 2005). Reducing the amount of information collected might not seem like a goal on which management is willing spend money. But consider the alternative. If a good way to quickly access requested information doesn't exist, then overly intrusive actions might have to be taken to ensure compliance with discovery requests.

### **Messaging**

It's difficult to determine which messages might be material to current or future litigation. Some organizations take a chance by relying on users for proper message management. IM communications are typically not captured at all. Both of these approaches put a company at risk.

It's important to be seen as taking a proactive stance in electronic discovery activities. The best approach is to archive all messages, including IM, without user intervention. Figure 1 is an example of a possible solution.

Email and IM messages pass through management systems that automatically intercept and write them to an archival storage system. Neither the sender nor the receiver plays any role in whether the information is archived. The archived messages are cataloged, indexed, and centrally managed according to the organization's records retention policy.

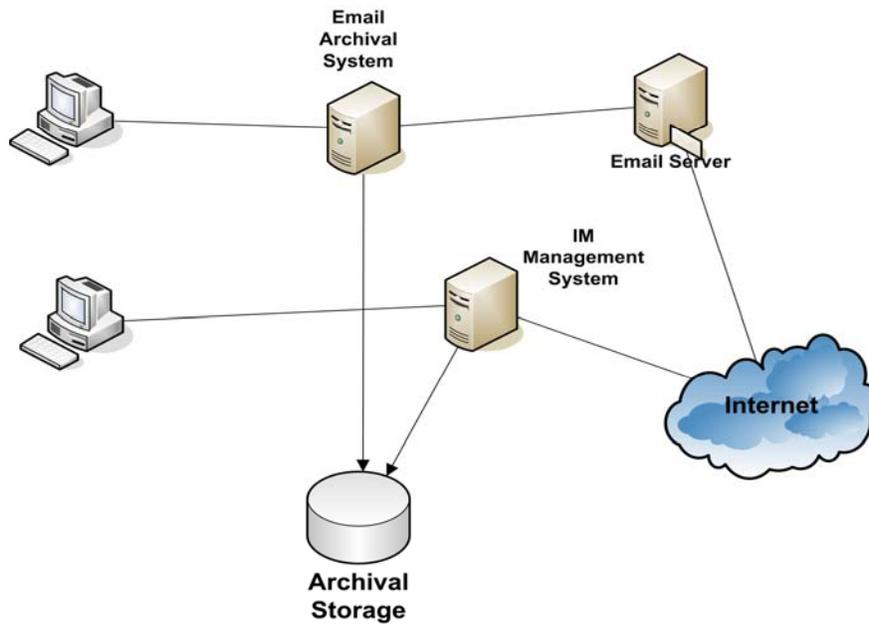


Figure 1

## Electronic Documents

As with messages, electronic documents must be preserved according to a company's records retention policy. They should also be available for discovery without significant cost. Deploying an electronic document archival system is a good way to meet these objectives.

Archival systems can operate automatically or with some operator intervention. In either instance, the system should be capable of enforcing business rules, including the imposition of litigation holds, related to document maintenance. Documents should be indexed, cataloged, and easily searched to reduce the effort required to produce information on any litigation issue.

## Justify your Solutions with Standards

Even if you purchase the best archival solutions possible, you're still missing one piece necessary to complete the electronic discovery puzzle. If called to testify or to be deposed, the questions will focus more on your company's practices and less on the solutions implemented (Flaherty, 2002). A good way to select justifiable processes is to follow a set of recognized best practices.

I'm not a strong advocate of blindly buying into a methodology. But there's value in adapting one or more industry recognized methodologies to create an electronic document and messaging management environment conducive to fair and cost effective discovery. At the very least, it makes it easier to justify the policies and procedures that resulted in the discovery results.

## Conclusion

As the amount of information stored electronically increases, so does the cost of providing that information during litigation. The old methods of allowing users to manage their own documents without the benefits of a central repository present too great a risk. As with all business processes, the management of electronic documents and messages should be approached in a way that minimizes risk to the business while keeping costs under control.

---

Copyright 2006 Thomas W. Olzak. Tom Olzak, MBA, CISSP, MCSE, is President and CEO of Erudio Security, LLC. He can be reached at [tom.olzak@erudiosecurity.com](mailto:tom.olzak@erudiosecurity.com) or by visiting <http://adventuresinsecurity.com>

---

## Works Cited

- CGOC (2005). *The Zubulake checklist*. Retrieved February 15, 2006 from [http://www.pss-systems.com/resources/zubulake\\_checklist.html](http://www.pss-systems.com/resources/zubulake_checklist.html)
- Flaherty, M.P. (2005, June). Would you please swear in the Chief Security Officer *SC Magazine*. Retrieved February 15, 2006 from <http://scmagazine.com/us/news/article/419805/would-please-swear-chief-security-officer/>
- Fulbright & Jaworski (2005). *Second annual litigation trends survey findings*. Retrieved February 15, 2006 from <http://www.fulbright.com/mediaroom/files/FJ0536-US-V13.pdf>
- Patzakis, J. (2006). Why the ediscovery revolution is important to infosec. *The ISSA Journal*, February 2006, p. 6.
- Roitblat, H. L. Ph. D. (2005, December). *Proactive solutions: the next generation of eDiscovery?* Retrieved February 15, 2006 from [http://www.discoveryresources.org/pdfFiles/Proactive\\_Solutions.pdf](http://www.discoveryresources.org/pdfFiles/Proactive_Solutions.pdf)