

Article

Document Retention Policies

A Lesson From Anderson: E-Mail Reveals!

One of the many lessons we've learned from the Andersen trial, with its focus on document shredding and the prevalence of such electronic evidence as emails, is not just the potentially incriminating nature of electronic archives, but the liability of inadequate enforcement of a document retention policy. It's one thing to have a policy; it's another to implement and audit it.



Develop, Enforce, & Audit Your Document Retention Policy

According to Lee Neubecker, President of Forensicon, a Chicago based security risk management and computer forensics firm that supports legal counsel in developing and auditing document retention policies for their clients, "companies, in anticipation of potential litigation, should have a document retention policy set up, and they need to operate within a policy created by their lawyers and to enforce it regularly, so that they can be certain they are operating within the realm of the law and protecting themselves from potential harm."

Not having a policy, or having one, but not acting on it on a regular basis is a problem, as was illustrated by the Andersen trial. As Neubecker explains, "if a document retention policy is acted on only before pending litigation, a company's actions may not hold up in court."

Preventive maintenance, including the education and training of employees on the policy, is essential to ensure the policy is enforced. "We work with management and counsel to test the effectiveness of the policy by conducting periodic searches of the data environment to see whether or not anything of interest turns up. If something

is found, counsel and the client discuss the ramifications and develop a strategy for dealing with that data or problematic behavior before anything gets to the point of litigation, so that the firm is protected and doesn't incriminate itself by keeping needlessly files that it has a right to dispose of."

Neubecker points out that he's not talking about destroying incriminating evidence or unethical behavior, but rather data that isn't official communication, such as working drafts, and day to day email with no future value, but he adds that "certainly, if you have anything that could be perceived as a 'smoking gun,' it is better to know about it, to minimize litigation risks." It's critical that companies know the contents and manage their information archives. Doing so forces employees to prioritize, to conserve network storage, and to conduct themselves ethically.

"If you have a policy, you need to audit it" Neubecker explains. "If you say these are things you do and don't do in email, how do you know employees are following the policy? Do you want to put your IT department in the difficult position of auditing and scrutinizing the integrity of their co-workers? You need to periodically pull in a third party firm to audit your adherence to your communications policies. Recent events and trends suggest that as firms get slapped with lawsuits, business leaders will appreciate the value of managing this risk. Insurance rates are going to go up, and eventually companies will be required to enforce and audit their document retention policies with third party risk management firms in conjunction with attorneys."

"Though this is a cost containment and risk management expenditure for corporations, businesses need to understand it is critical one," Neubecker cautions, "because the costs of not developing, enforcing, and auditing a document retention policy could be devastating."