

Corporate Governance – The Impact on Your IT Staff

By Jeffrey Plotkin
Attorney at Law

September 5, 2003

Compliments of



Corporate Governance – The Impact on Your IT Staff

By Jeffrey Plotkin
Attorney at Law

Jeffrey Plotkin is a partner of the New York City law firm of Eiseman, Levine, Lehrhaupt & Kakoyiannis, P.C. Mr. Plotkin formerly was Assistant Regional Administrator of the Securities and Exchange Commission's New York Regional Office.

1. Introduction

The federal securities laws do not impose affirmative requirements on public companies to retain their e-mails. Nonetheless, prior to 2002, many public companies, either as a matter of sound corporate practice, or because of particular regulatory requirements applicable to their business, adopted and implemented comprehensive e-mail retention/destruction policies.¹

In 2002, President Bush signed into law the Sarbanes-Oxley Act. This legislation was designed to enhance corporate governance standards, by, among other things, enhancing corporate accountability, tightening securities disclosure requirements, increasing regulatory oversight of auditing firms, and creating new federal crimes and increasing penalties for existing federal crimes.

As discussed below, Sarbanes-Oxley, and the SEC rules promulgated thereunder, should definitively persuade all public companies to institute and adhere to systematic e-mail retention/destruction policies with respect at least to certain key business units and categories of personnel.

In fashioning appropriate e-mail policies in response to Sarbanes-Oxley, management should be mindful of the technical capabilities of the company's IT Department and existing computer infrastructure, and the substantial burdens and strains that comprehensive e-mail policies can place on an IT Department, particularly in larger, more diffuse corporate environments.

This paper discusses various considerations that should be taken into account in developing adequate e-mail retention/destruction policies, and the alternatives available to minimize the impact of such policies on the IT Department.

2. Sarbanes-Oxley Demands Prudent Record Retention Policies

Under Section 802 of Sarbanes-Oxley, you can be sentenced to prison for up to twenty years for deleting an e-mail "in contemplation" of a federal investigation or "matter" that does not yet exist, if a jury is convinced that your intent was to "impede, obstruct or influence" such possible, not-yet-commenced, matter.²

Presuming the inevitability of a federal investigation into the financial activities of any large public company, a company employee who deletes what he perceives to be a troublesome e-mail message, years in advance of a possible investigation, may subject himself to criminal prosecution, even if turned out that the deleted e-mail would have been of no actual importance to the investigation.

In light of this new sweeping criminal provision, companies would be well advised to implement policies that mandate retention of e-mails from specific business units or categories of key employees, mandate lengthy retention periods for such e-mails, and set forth specific destruction protocols. Companies must be vigilant in educating their employees about their policies, and stressing the implications arising from non-compliance with those policies.

Of paramount importance is the need for a company to consistently apply and adhere to its retention policies across all business units and categories of key employees. In particular, when a retention period for a particular record has lapsed, that record should be destroyed promptly as provided by the policy. If a record is not destroyed at the required time, but is destroyed later on an apparently arbitrary basis, the company and its responsible employees will find themselves on the hot seat if the records coincidentally were destroyed on the same day an SEC subpoena was delivered to the company's General Counsel.

Of course, a company's policy should mandate that no employee erase any e-mail except in accordance with the policy. However, a company should not allow employees even to be in a position to attempt to erase the only record of a business-related e-mail that could be relevant to a future federal investigation. Instead, the company's policy should mandate that all e-mails (including instant messages, and e-mails from employees' laptops, cell phones, PDAs, and home computers, if plausible) be captured, routed, preserved, and retained in a central archive location in a non-alterable, non-erasable format for an appropriate time period.

And in crafting an e-mail policy, the retention periods for e-mails may well vary for different business units or categories of key employees. The retention periods should be tailored, if possible, to (1) applicable regulatory requirements, (2) relevant criminal and civil statutes of limitation, (3) duration of material contracts (for which negotiations and revisions were handled via e-mail), (4) the commercial needs of the business units, (5) the company's past experience with respect to the need to maintain correspondence, and (6) the possibility that correspondence on certain subject matters may become relevant in the future (e.g., for civil litigation purposes).

A company's policy also should require that notification be made to designated management personnel upon any employee's or attorney's receipt of any regulatory request, subpoena, or notice of possible lawsuit, so that regularly scheduled destruction of documents pursuant to the policy may be halted, if necessary, in light of the nature of legal developments. The IT Department should have the capability to quickly prevent

regularly scheduled destruction of documents that possibly could be relevant to an investigation or litigation.

3. IT Department Concerns

Management should work closely with the company's IT Department to determine the technical feasibility of implementing broad e-mail retention/destruction policies as described above.

For instance, if it is not feasible to capture on the company's servers e-mails exchanged from outside e-mail systems utilized by employees, the firm's policy should prohibit business e-mail from such outside e-mail systems.

Also, management should work with the company's IT Department to determine the financial burdens of storing, and preserving the integrity of, a potentially huge volume of electronic data. Companies have two alternatives in achieving compliance with e-mail retention policies. They either can attempt to build or revamp their own electronic retention systems in-house, or utilize the services and products of established outside vendors. The latter approach would make economic and business sense for most companies.

For instance, software vendors have designed programs that allows companies to:

capture and journal in "real-time" all e-mails (including "instant messages") and attachments to a central archive that stores the records in a non-erasable, non-alterable format until expiration of the retention period;

access and manage the archived e-mails via a user-friendly web interface; and

implement structured review processes to search, sample and review journaled e-mail to efficiently respond to discovery demands made by the authorities, or by parties in civil litigation. For instance, the company may define the scope of an e-mail review by specific criteria (e.g., date range, sender/recipient lists, internal and/or external e-mail, and text content search).

Companies that take advantage of such third-party software may significantly reduce their costs and anxieties related to necessary e-mail retention/destruction policies.

4. Particular Focus Areas for E-Mail Retention

In determining which key business areas, and/or categories of key employees should be subject to e-mail retention policies in light of Sarbanes-Oxley, companies should focus particularly on directors who serve on the audit committee, senior executive officers who provide certifications on the company's quarterly and annual filings, internal audit personnel, and other management and accounting personnel who communicate with outside auditors.³

By way of example, Section 303 of Sarbanes-Oxley, and amended SEC Exchange Act Rule 13b2-2 promulgated thereunder, make it unlawful for any officer or director to take any action to fraudulently influence, coerce, manipulate, or mislead any auditor engaged in the performance of an audit of the financial statements of the company for the purpose of rendering the company's financial statements materially misleading.

Therefore, during any financial accounting fraud investigation, the SEC and criminal prosecutors would be particularly interested in reviewing e-mails of those persons who had any communications with outside auditors, including senior management and members of the board who serve on the company's audit committee.⁴

Indeed, Sarbanes-Oxley Section 802, and SEC Rule 2-06 promulgated thereunder, makes it a crime, punishable by up to ten years in jail, for auditors of public companies to fail to maintain for a period of seven years all correspondence created, sent, or received "in connection with an audit or review" of a public company, including any "electronic records."

It is perfectly conceivable then, that criminal prosecutors would view a public company's deletion of e-mail correspondence with its auditor (particularly if the auditor deleted the same correspondence) as a violation of Sarbanes-Oxley's records tampering provisions discussed earlier in this paper. The prosecutors would argue that a reasonable person should "contemplate" that prosecutors will subpoena such e-mails in any prospective investigation into possible accounting irregularities, and the company's destruction of such records must have been undertaken purposefully to obstruct such prospective investigation, or in reckless disregard of the fact that such an investigation was inevitable.

A prudent company would therefore be well advised to adopt procedures requiring that e-mail correspondence with auditors be maintained for a period of seven years -- the same time period that auditors are required to keep those very same e-mails.

5. Conclusion

Given the uncertainty that exists with respect to the scope and interpretation of Sarbanes-Oxley's criminal provisions for record tampering, public companies should take all steps necessary to ensure that no federal prosecutor be left with the impression that company e-mails were deleted other than in connection with a reasonable, predetermined, and systematic retention/destruction policy.

The costs of implementing and complying with appropriate e-mail policies are substantial. However, the alternative of doing nothing will prove more costly in both human and financial terms. To control costs, companies should utilize all available technologies to assist their IT Departments in ensuring compliance with their e-mail retention/destruction policies.

¹ For instance, broker-dealers registered with the SEC must keep e-mail correspondence for a period of at least three years. See generally, Jeffrey Plotkin, *Broker-Dealer Regulations Concerning E-Mail*, New York Law Journal, December 4, 2002.

² See 18 U.S.C. 1519:

Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both. (Emphasis supplied).

See also 18 U.S.C. 1512, that was amended pursuant to Sarbanes-Oxley:

(c) Whoever corruptly--

(1) alters, destroys, mutilates, or conceals a record, document, or other object, or attempts to do so, with the intent to impair the object's integrity or availability for use in an official proceeding; or

(2) otherwise obstructs, influences, or impedes any official proceeding, or attempts to do so,

shall be fined under this title or imprisoned not more than 20 years, or both.

³ Putting aside Sarbanes-Oxley concerns, a public company would be well advised to retain e-mails from other business units, including, but not limited to, the investor relations department (e.g., to monitor compliance with SEC Regulation FD) and the human resources department (e.g., with respect to statutory discrimination claims by employees).

⁴ Pursuant to Sarbanes-Oxley, the audit committee is "directly responsible for the appointment, compensation, and oversight of the work of any registered public accounting firm employed by that issuer (including resolution of disagreements between management and the auditor regarding financial reporting) for the purpose of preparing or issuing an audit report or related work, and each such registered public accounting firm shall report directly to the audit committee." See Section 10A(m)(2) of the Securities Exchange Act (emphasis supplied).