

## Feature Article

## A Risk-Based Approach to Email Management



Jon Neiditz



Jonathan Bank

by Jon Neiditz and Jonathan Bank

The ever-growing focus on emails in investigations and litigation, together with increasing e-discovery costs and spoliation sanctions, have led many of our insurer and reinsurer clients to focus on how they are managing email retention. When they do, they often find challenges in assuring compliance with their complex recordkeeping requirements and records management policies, as they relate to electronic documents, and particularly to “unstructured” documents like emails.<sup>1</sup> We are also seeing that these documents are becoming

**Unstructured emails pose greater challenges because they (1) are much more likely to fall into multiple categories, (2) are written much more easily... and (3) are disseminated much more widely...**

the repository of information, both business-critical and sensitive. Emails have, in many instances, taken the place of short telephone conversations, replacing a largely undocumented form of communication with an indelible record of what was said.

Approaching records management and email destruction programs with these major risks in full view focuses the mind. Records management programs have generally been driven by regulatory retention requirements with every category of document being assigned a number of years of retention. This approach to records management generates a highly detailed schedule for all companies that face complex regulations of their businesses, including not only insurance regulation but areas such as environmental, human resources, benefits and payroll documents. However, with a relatively very

*Mr. Neiditz is Of Counsel in the Atlanta office of Lord, Bissell & Brook and can be reached at [jneiditz@lordbissell.com](mailto:jneiditz@lordbissell.com). Mr. Bank is Of Counsel in the Los Angeles office and can be reached at [jbank@lordbissell.com](mailto:jbank@lordbissell.com).*

small percentage of paper documents falling into ‘boilerplate’ categories, it was historically relatively easy to determine that a document fell into one and only one category, and to retain such documents for only the number of years required.

Unstructured emails pose greater challenges because they (1) are much more likely to fall into multiple categories, (2) are written much more easily so that there are vastly more of them, and (3) are disseminated much more widely to many more recipients and are much more easily saved by direct and indirect recipients (particularly prospective plaintiffs). The third point is the critical one; in litigation and investigations, the only safe assumption may be that once an email has been written it cannot be destroyed; and it may emerge as a “smoking gun” at precisely the wrong point in litigation — not only regardless of your destruction policy but because of that policy — for had you not destroyed the email and known about it, it would be far less lethal. Moreover, the risks associated with these “smoking gun” emails is generally far greater than the risks associated with failure to comply with regulatory retention requirements.

Until recently, email destruction programs were most often established by IT departments with storage costs in mind. Obviously, the 30-, 60- or 90-day email destruction policies that emerged do not comply with regulatory retention requirements in a legal environment in which emails are “documents” subject to those differing and various requirements. But even aside from those contradictory policies, any tech-savvy investigator or plaintiff knows that electronic storage costs have been dropping precipitously — an average of 38% a year over the past four years.<sup>2</sup> In this cost environment, now that emails are also known to be central to most corporate investigations and litigation, companies may become concerned that a rigid and quick email destruction policy — even one that complies with regulatory retention requirements — may be viewed as an effort to obscure business practices that do not meet the highest standards.

Thus, the benchmark of a good electronic document

*continued on page 23*

## Feature Article

**Email Management...**

continued from Page 11

retention program today cannot be simply that it complies with regulatory timeframes, and/or that it reduces electronic

... a good electronic record retention program must properly balance risks and costs in the new legal landscape for emails and other unstructured data such as instant messaging, SMS messages and voicemail.

storage costs. At a minimum, a good electronic record retention program must properly balance risks and costs in the new legal landscape for emails and other unstructured data such as instant messaging, SMS messages and voicemail.

Based on the unfortunate recent experiences of companies like UBS and Morgan Stanley in finding and restoring backup tapes, all companies are well-advised now to consider using backup tapes only for disaster recovery purposes, rather than for archiving and retrieval. But that conclusion only begs the question of what kind of archiving will be most useful. For example, what search capacities will make an electronic archive most useful for day-to-day retrieval, and will best manage costs in litigations and investigations? And how should your archiving choices influence your choices for filtering incoming emails?

Recognition that casual emails are creating immense risks for companies is also leading many companies to focus on preventing the problem. Policies and training on responsible use of emails are nothing new: however due to emails' 'false sense of privacy' and ease of use, those policies and trainings are often ignored. Along with tighter policies and training that makes the magnitude of the risks clear, we are seeing a trend toward (1) more stringent sanctions, consistently applied, (2) more regular monitoring of employee emails and (3) more specific company-wide notice of that monitoring. Recent results of a survey indicate that 25% of U.S. employers acknowledge having terminated employees for misuse of the email system. 55% of U.S. employers retain and review emails, and over 80% indicate that they notify employees of web monitoring, email monitoring, company storage, review of computer files and monitoring content, keystrokes and time spent online.<sup>3</sup> Increased focus on controls as a result of Sarbanes-Oxley, and a desire to make all compliance programs satisfy the U.S. Sentencing Guidelines' standards for compliance programs are major drivers of these developments.

Control of your email is increasingly central to control over your information, including the ability to defend yourself and assert your rights. Your IT and records management experts must come together with your legal, financial and claims departments to take on this challenge. And remember, when you want to "reach out and touch somebody," you still have a telephone...wireless no doubt. ■

## Notes:

- 1 "Structured" documents are made up of elements that readily fall into classifications that can be queried, searched and sorted automatically, whereas in "unstructured" documents, such as emails, words and numbers are not inherently tagged with machine-readable significance, posing a challenge for electronic records management systems.
- 2 IDC reported that the dollar-per-gigabyte price of external disk storage was down 36% in 2004, 33% in 2003, 40% in 2002 and 43% in 2001. Lucas Mearian, Computerworld Hong Kong Daily, March 7, 2005.
- 3 American Management Association/ePolicy Institute 2005 Electronic Monitoring Survey, May 2005.

## Feature Article

**Regulatory Supervision...**

continued from Page 21

should only be approved if they do not conflict with the regulator's plan. Moreover, if there are numerous requests for variances, it suggests that the company's plan is not feasible and needs to be revised or abandoned.

One of the dangers of supervision is the proximity of the supervisor to the company. Often, the supervisor resides at the company throughout the period of supervision. This may cause the supervisor to become more casual in reviewing decisions because the supervisor may assume that he or she has a complete understanding of the company. Supervisors should continue to require formality in the approval of all material transactions. There have been several instances where receivers have attempted to renounce transactions approved during supervisions that turned out to have been based on inadequate or misleading information.

**Conclusion**

Supervision provides regulators an opportunity to intervene in a company's affairs without displacing management. Supervision used in conjunction with a run-off plan provides an opportunity to wind up the affairs of a company without the need for receivership. But it also presents challenges and hazards to the regulator if it is not properly conducted. ■