

The Danger of Short Email Retention Strategies

by Thomas Bookwalter, CEO FMDC

The number of companies that still believe that a short email retention strategy is good business is surprising. What is more surprising is the number of attorneys that still recommend deleting emails rather than managing them. The notion is, "If I don't have it, I cannot produce it and so I am not at risk." There are several flaws to this argument.

- 1) Just because you do not have it, does not mean it does not exist. If an email becomes the focus of litigation or investigation, then not having the record is worse not better. The implication is that it was deleted because it was damaging and that its deletion was part of a cover-up. Courts have instructed jurors to assume that because records cannot be produced, the records must be damaging to the respondent. Under Section 1519 of Title XVIII of the US Code, it is a felony punishable by up to 20 years imprisonment for anyone to destroy, alter or make records inaccessible in matters relating to the activities of US government agencies. It applies to anyone that tampers with records, not just executives of public companies.
- 2) Delete does not always mean delete. Emails have a life of their own. At companies with short retention policies employees make their own copies, storing their emails in .pst or .nsf files on their desktop and laptop computers. If there is a concern that an email might become a point of contention, sometimes the email is sent to personal email accounts outside the company or even to a friend.
- 3) Court rulings have not been sympathetic to people that destroy potential evidence whether by accident or by policy. Just because a company has a written plan to remove records that should have been kept, is no excuse. An ever-increasing number of court cases strengthen the obligation in the eyes of the courts that the records must be kept and penalizes those that ignore the requirements.
- 4) Regulators have become intolerant of companies that flaunt their obligation to preserve and produce records when asked. Companies are being fined for failing to keep records according to regulatory standards; not just because of retention periods but also because of failure to meet the other requirements of the rules.
- 5) Often companies that delete emails from mail system mailboxes have copies of those emails on backup tapes. The cost to retrieve those emails is staggering. The cost of retrieval in a case or investigation can easily exceed the cost of an entire email archive system.
- 6) If investigators suspect or opposing counsel can prove that emails may exist on desktops and/or laptops, courts have ordered that the systems be confiscated or that opposing counsel be given access to do its own searches.
- 7) Email is not a type of record. It is a mail delivery system; like the US mail. It is the contents of the message that determines its retention, not how it was sent.

On the surface, deleting emails quickly or after only a short retention period appears to be a clever way to avoid email risk. It is only on the surface. A closer examination of the facts reveals that deleting emails before their time increases risk and expense.

PROTECTING ENTERPRISE VALUE

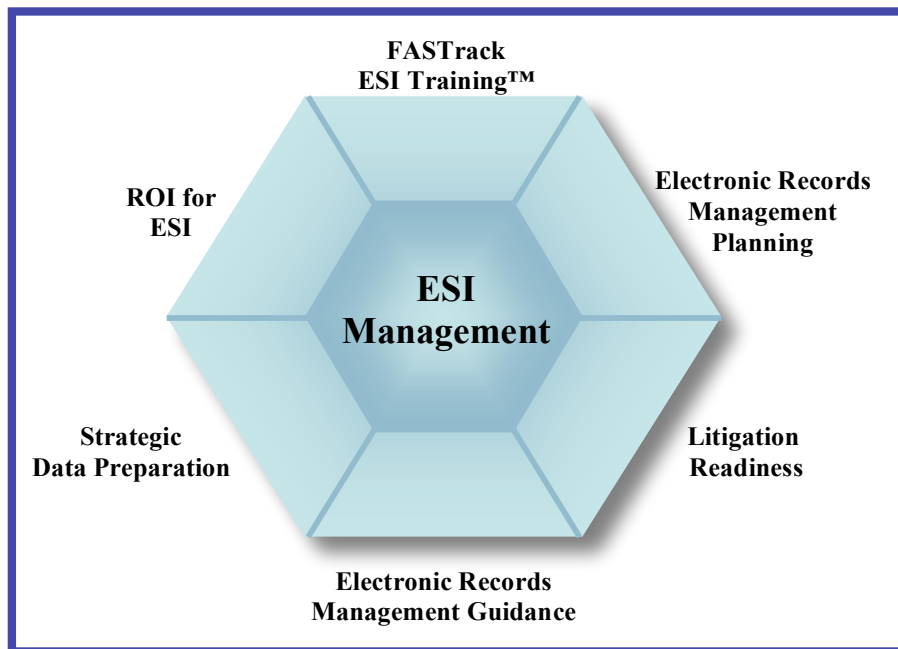
#9. The Danger of Short Email Retention Strategies

About FMDC

Founded in 1987, FMDC has focused on the issues relating to the processing and management of information in regulated environments. Since its inception, FMDC has been at the nexus of regulation, industry and information technology. With projects in over twenty countries, FMDC professionals have gained first hand knowledge of the nuances of the different regulatory jurisdictions and how they impact the use of technology. In early 2002, FMDC turned its attention to the issues relating to the handling of e-mail, instant messaging and other records in the context of regulatory requirements and litigation.

The advent of laws and rules such as SEC Rule 17a-4, the Sarbanes Oxley Act, State and Federal privacy legislation, industry standards such as PCIDSS and most recently, court rules or guidelines such as FRCP, CCJ-ED, local federal district rules and the Sedona Conference has changed the standards by which companies must manage their information. FMDC professionals work to guide companies through the morass of regulations to find cost effective solutions for the management of ESI. Our services include:

- FASTrack ESI Training™
- Electronic Records Management Guidance and Policy Development
- Strategic Data Preparation
- Litigation Readiness
- ROI for ESI
- Electronic Records Management Planning



If you are concerned about ensuring that your ESI management meets your business, litigation and regulatory obligations or if you must find ways to reduce the associated costs contact FMDC.

Western US Region

Joseph Santoro, VP
Newport Beach, CA
949 231-9602

joseph.santoro@fmdc.com

CEO

Thomas Bookwalter
Santa Fe, NM
908 812-5000

thomas.bookwalter@fmdc.com

Eastern US Region

Michael Shope, VP
Middletown, NJ
732 687-2680

michael.shope@fmdc.com