

## **Plugging the Leaks**

**by Thomas Bookwalter, CEO FMDC**

Corporate information is precious. Customer databases, product performance records, business plans and marketing strategies, customer proposals, trade secrets, product designs are substantial corporate assets. They are hard to count, but in the hands of a competitor they can be damaging.

Corporate espionage has become an advanced science as competitors strive to find advantage by any means. In the 2003 CSI/FBI study on business information loss, 251 companies reported that loss of proprietary information accounted for over \$70,000,000 in losses. It was the highest loss category accounting for over 34% of the total losses reported.

Much of that information leaked through email.

Email has become a focal point for information management challenges for companies. Not only is email one of the ways that proprietary information leaks out of companies but also, email is one of the ways that information spreads improperly within a company. Not everyone should have easy access to all of a company's information. In some cases, laws prohibit such access. For example, the Health Insurance Portability and Accountability Act (HIPAA) has strict requirements for the management of health information. Companies that offer health insurance to their employees must take care that emails discussing employee health matters are kept private and confidential.

The Financial Modernization Act of 1999, commonly know as the Graham Leach Bliley Act or GLBA, has requirements for maintaining the privacy and confidentiality of customer financial information. When emails are used to discuss these and other matters of a confidential nature, it becomes necessary to create safeguards that help prevent the inappropriate use of the information.

Companies that follow a laissez-faire approach to email management encourage disregard for the importance of information privacy and invite risk and liability. Email is an integral part of modern business. Surveys indicate that as much as 90% of a company's business communications are via email or its counterpart instant messaging. The nature of email is casual. Business communications are mingled with idle chat among colleagues. This Jekyll and Hyde quality fosters its use and treatment in a casual way.

Make no mistake, email is a business resource and must be managed as a business asset. Employees should be aware of a company's guidelines for use. Companies should be diligent in managing the email environment. Critical data should be protected from export or internal movement by appropriate content filters and access controls. Audit trails and archives of email activity should be maintained so that when there is concern that email is being used improperly, it can be investigated and validated. Email archiving should be an integral part of an email management strategy. Not just because regulations require it, but also to protect the enterprise. Protect your company. Make your email tamper-proof and leak-proof.

## PROTECTING ENTERPRISE VALUE

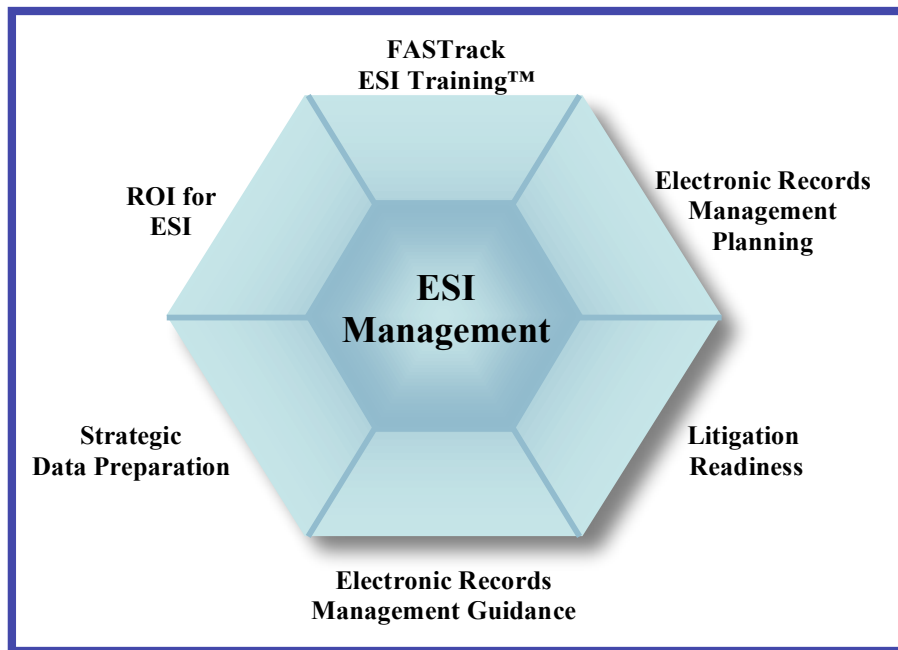
### #3. Plugging the Leaks

#### 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](mailto:joseph.santoro@fmdc.com)

**CEO**

**Thomas Bookwalter**  
Santa Fe, NM  
908 812-5000

[thomas.bookwalter@fmdc.com](mailto:thomas.bookwalter@fmdc.com)

**Eastern US Region**

**Michael Shope, VP**  
Middletown, NJ  
732 687-2680

[michael.shope@fmdc.com](mailto:michael.shope@fmdc.com)