The Need for E-legal Compliance

An EOIF Presentation

EOIF Organization

- Electronic Original Initiative Foundation
- Non-for –profit body
- Based in Washington with sub offices in Europe and Australia
- Full time CEO
- Industry Associations
- Commercial Sponsors
- Advisory Body and Review Board (BSI)

Electronic Original Initiative Foundation (EOIF) Objectives

- Establish Standards
- Promote case for e-legality
- Engage with Government
- Work with regulatory bodies
- Promote Standards for customer protection

Commercial Sponsors

- Storage - HP and Network Appliance
- Archiving - Legato and Veritas
- Signatures – Verisign and Identrus
- Doc Mgmt – Filenet
- E-commerce - Commerce One
- Accounts – Sage
- Majors - Microsoft
- Service Providers – Bytes and Zantaz
- Consultants – Kahn Consulting

Industry Associations

- Standards – BSI, NIST, Open Group
- Regulations – SEC, HIPAA, FDA, OCC
- Industry NCHICA, Phrma, SIA
- Storage, and Doc Mgmt – SNIA/SNIF, ARMA
- Messaging - EEMA/ECAF
- Commerce/AccountsIFAC,AICFA,Commercenet
- Users , lawyers - ITAA, ABA
- Plus European and Asian counterparts

Key E-Legal Issues

- Duty of Care records retention
- Financial records retention
- Evidence

Duty of Care Requirement

- To keep key company records for 5-7 years
- 80% of B TO B communication is e-mail
- Less than 1 in 5 companies are currently keeping e-mail beyond 1 year
- In some cases Board Directors are personally responsible

Financial records retention

- Will be communicated 80% electronically by 2010
- 72% of organizations already sending some electronically
- Only 1 in 5 keeping beyond 1 month
- Audit and retention issue
- Sarbanes Oxley Act

Evidence

- Need to be Discovery Order ready
- Need to decide what to keep and delete
- Needs document policies and standards
- Evidence mail - Merrill Lynch $1.5 billion
- Enron,Worldcom, Arthur Anderson, Tyco

Special Industry Regulations

- Examples SEC, HIPAA, Pharmaceutical
- Don’t often cover technical and operational requirements
- Don’t cover other general requirements eg Duty of Care,Financial records
- Are national not international

Engage with Government & Regulatory Bodies

EOIF's Role includes:

- Compliance issue
- Faulty legislation
- Harmonize standards and regulations internationally

Financial Regulations

Compliance with NASD and SEC regulations starts with Codes of Conduct - NASD 2210 - Defines rules of conduct for all communications with public (advertisements, sales literature, correspondence)

2. Retention (SEC 17a-4, NASD 3110)
   - All security brokers and dealers to maintain records of business and customer account information with easy access
   - Electronic storage must be in WORM format and accessible for checking compliance
3. Supervision (NASD 3010)
   - Effectively monitor correspondence, show adherence to codes of conduct.
   - Record supervisory activity itself

Other Regulations

Sarbanes-Oxley Act

- Passed in July 2002 in direct reaction to accounting scandals of late 2001 and 2002.
- Among other things, the Act focuses on retention periods and standards for the documentation (including email) surrounding an audit.
- Protects investors by improving accuracy and reliability of corporate disclosures made for securities laws (& other purposes)

HIPAA (U.S. Heath Insurance Portability and Accountability Act)

- Requires healthcare-related organizations to protect security and confidentiality of electronic patient information.
- Includes test results, x-rays and email correspondence between doctors, patients, pharmacists, etc.
- Covers health plans, payment clearinghouses and electronic business partners that maintain or transmit electronic patient information.

Other Regulations

Department of Justice Freedom of Information Act (FOIA)

- The Freedom of Information Act (FOIA) was signed into law in 1966 and provides that any person has the right of access to federal agency records or information.
- The DoJ is required under the FOIA to disclose records requested in writing by any person.

Record Management Challenge: Risk Management

34.5% of organizations say they could not recover emails if required for legal or regulatory discovery within next 12 months. (CNI, 2000)

- 83% of lawyers say their corporate clients are NOT prepared to retrieve and turn over electronic files. (Arthur Anderson, 2001)
- 49% of organizations have established policies regarding email retention …BUT 41% of users ignore the policy. (CNI, 2001)
- 87% of viruses enter via email. (2000 Virus Prevalence Survey, ISCA))

Record Keeping System Requirements

- To build record keeping into corporate messaging systems…
  - Microsoft Exchange
  - Lotus Notes
- What is needed?

- ✓ Authenticity
- ✓ Usable Evidence
- ✓ Completeness
- ✓ Management
- ✓ Retention schedule
- ✓ Training
- ✓ Chain of custody
- ✓ Auditing
- ✓ Accessibility
- ✓ Indexing
- ✓ Security

Authenticity

- Challenge
  - ✓ Record must be maintained as authentic and ‘unalterable’ from creation through disposition.
  - ✓ Lotus/Messaging don’t include controls on access, editing of stored messages.
- Response
  - ✓ Capture and store records directly from message store
  - ✓ Verify accuracy of storage process
  - ✓ Support reliable and (optionally) indelible media (WORM, etc)
  - ✓ Audit all access to records.

Usable Evidence

- Challenge

  Overcome legal objection

  - Routine creation
  - Document a normal business activity
  - Created when the underlying event took place

- Response

  - ✓ Capture incoming and outgoing email messages at time of creation or receipt
  - ✓ Retention rules applied systematically
  - ✓ Application of a file plan (categories) with policies and retention schedules.

Completeness

- Challenge
  - ✓ Record integrity depends on three attributes: content, context, structure.
  - ✓ Moving messages out of mail servers typically changes one or more of these attributes. (loss of email meta-data)
- Response
  - ✓ Save complete email record and attachments in native document format.
  - ✓ Save meta-data as part of record.

Management

- Challenge

  Corporate email systems do not recognize:

  - ✓ Value-based email management. Record vs. non-record.
  - ✓ Creating, maintaining record categories.
  - ✓ Managing retention of record series.

- Response

  - ✓ Record declaration integrated to email client
  - ✓ Rules-based record classification
  - ✓ Presentation of file plan as part of MS-Exchange or Lotus Notes folder structure.
  - ✓ Retention integrated into message stores.

Practices & Training

- Challenge
  - Match rigor of record-keeping science to ubiquity of email within business/government user community
  - Integrate record management with IT practice.
  - Apply record-keeping to build business value.
- Response
  - Build record-keeping into email client, present file plans as part of Outlook/Notes folder structure.
  - Integrate retention into message stores/databases.
  - Use volume and availability of email
    - Build e-business programs on email
    - Re-use email as corporate memory.

Auditing

- Challenge
  - ✓ Little to no audit/control of message storage and access in MS-Exchange or Lotus Notes.
  - ✓ Messages and documents easily move from clients to server databases, personal archives, and backup tapes.
- Response
  - ✓ Audit message/record access.
  - ✓ Integrate “chain of custody” controls into message stores of MS-Exchange and Lotus Notes.

Accessibility

- Challenge
  - Message access in Exchange/Notes largely based on visual markers.
    - Inbox
    - Folder structure
  - Full text index is very ‘resource-expensive’ in Notes, and non-existent in MS-Exchange.
  - Users have limited access to long-term message stores (backup tapes, archives).
- Response
  - Use full-text index for secure user access to “corporate memory”
  - Present corporate file plan as a common folder structure.
  - Use SQL database for programmatic access.

Security

- Challenge
  - Messages often not secure in typical messaging system.
    - User archives.
    - Backup tapes.
    - Un-audited message stores.
  - SMTP traffic can be seen in clear text (not encrypted)
- Response
  - Build practices, systems to control all access to message stores.
  - Integrate messaging directories into record-keeping system.
  - Adopt privacy policies, solutions for secure messaging (encryption)

EOIF Summary

- There is a major need to establish international standards for record management
- Wide Support needed from all parties
- Govt and Regulator and consumer Benefits