HYDER & ASSOCIATES
MANAGEMENT REPORT

Volume XIX Number II Spring 2008

ELECTRONIC DISCOVERY

Federal Rule of Civil Procedure 30(b)(6), as well as corresponding state rules, are the new "weapon of choice" in the battle for electronic discovery, and IT directors and RIM managers are in the cross-hairs of the controversy. Rule 30(b)(6) requires a company faced with electronic discovery to designate one or more officers, directors, managing agents, or other persons to testify under oath as to matters known or reasonably available to the organization, e.g., information management and document retention. Depending upon the counsel's goal and strategy, the questioning may be used for routine information on gathering or rather it may be aimed at uncovering intentional or negligent spoliation of data potentially relevant to the litigation.

The following questions are designed to uncover how records and information management processes work within your company and to determine how effectively they operate on a day-to-day basis, RIM managers would do well to notice that electronic records are emphasized and that answers to the questions could be very complex for large companies with highly decentralized operations.

NORMAL COURSE OF BUSINESS DOCUMENT AND DATA RETENTION QUESTIONS

Typical General IT Questions

- In how many different locations do you have operations?
- Where are they located?
- How many severs does your company use?
- Are all servers backed up for disaster recovery purposes?
- Can you identify which server(s) support each application?
- Can you identify which back-up tapes contain data from a selected server?
- Can you identify which IT assets (hardware and software) are being used by each employee?
- Is there a published set of IT compliance rules? Is the document available?

Data Retention Questions

- Who is the person in charge of your data retention policies?
- Are this person's responsibilities regional, national, and/or international?
- Are the data retention policies published and is the document available?

- Do you always follow the published data retention policies? If not, why not?
- Are you aware of the regulatory rules concerning document retention for your organization (SOX, SEC, HIPAA, etc.)?
- How long has it been since the data retention policy has changed?
- Has the policy changed as a result of any pending legal

continued on pages 2 & 3

INSIDE

COMPLIANCE CORNER

Nearly Half of U.S. Workers Feel Bullied at Work…*And They Want to Sue*

More than 44 percent of 534 U.S. workers surveyed feel that their bosses bully them on the job, according to the Employment Law Alliance, a San Francisco-based network of employment and labor attorneys. The survey also found that 64% of workers feel they should have the right to sue if bullied. Bullying bosses are those who publicly criticize, rudely interrupt, tease, give dirty looks, use sarcastic jabs, or flat out ignore certain employees, according to the survey's respondents.

Since it is difficult to characterize bullying, juries would have a tough time legally defining the problem, according to Stephen Hirschfield, CEO of the Employment Law Alliance. Hirschfield said he was also surprised at how many workers would consider litigation, adding that he does not feel courts should be addressing the problem, because such cases would put "the jury in a situation where they have to Monday morning quarterback."

Hirschfield suggested that companies change their sexual harassment policies in order to include the most common bully tactics that bosses seem to use. It would put management on notice of what is acceptable and what isn't. The policies should have a zero tolerance policy for those problems.

Bullying is a deliberate campaign to destroy somebody else's job or career. The problem is most people do not realize that bullying is an issue. Business owners should look at turnover rates and absenteeism numbers. If people in a certain division show a tendency to not come to work, then the division head may have pushed the employees to the extreme measure of avoiding the job altogether.

Source: HR Fact Finder, February 2008

DID YOU KNOW?

- Recent surveys have shown that an average U.S. company faces 305 lawsuits at any one time, and large firms with $1 billion or more in revenue deal with 556 at once.
- 95% of all business communications today are created and stored electronically.

Source: The Information Management Journal, July/August 2007

ELECTRONIC DISCOVERY

continued from page 1

actions?

- Is this retention policy in place across all locations within the company?
- Has this been audited across the company? When and by whom?

E-Mail Questions

- What is the current retention policy as to electronic documents and other data?
- What e-mail systems are you using? What versions?
- Who is the person(s) in charge of the company e-mail systems?
- Are all sites using the same e-mail package and version?
- What other e-mail packages have you used historically?
- When did you migrate from the previous version to this version? Over what time frame?
- Were all sites using the same package at that time?
- Were the old mail boxes converted or did the users simply have an old and new mail box?
- What happened to the old e-mail? Was it deleted or allowed to stay on the server?
- Do those servers still exist?
- Were the disks ever imaged or copied other than to tape?
- Does that media still exist today?
- Can a user have multiple e-mail accounts?
- How are these accounts tracked?
- Where is e-mail saved when a user saves it?
- Does the user have options as to where to save e-mail? What are the options?

Tape Backup Questions

- What backup systems are you currently using?
- How long have you been using them?
- Is the same version in use across all sites? If not, why not?
- What other systems have you used historically?
- When you migrated from one system to other system, what happened to the old data?
- What types of storage media are you currently using?
- Are all sites using the same generation of technology?
- What other types of technology have been used historically?
- When you migrated from the older technology to the new technology, what happened to the old tapes?
- Did you retain the old tape drives and software to allow access to this technology?
- How do you keep track of which tapes you own and which tapes are onsite or offsite?
- Have you always used this system? If not, what system was used previously, and how was the information migrated

continued on page 3

continued from page 2

when the new system went into place?

- When you move a tape offsite, how do you reconcile the media move?
- How often do you perform a physical media audit to ensure that all tapes are accounted for?
- How is your media stored?
- Is it on a rotation cycle?
- How is the cycle determined?
- Do you have a policy of verifying that backups are accurate?
- Have you ever stored data onsite?
- If you now store data offsite, have you physically audited these old locations to ensure that they no longer contain media of any kind?
- Who is your offsite storage vendor?
- How long have you used this vendor?
- Do all sites use the same vendor?
- What other vendors have been used historically?
- Have you performed an audit to ensure you have the data you think you have?
- Do you maintain historical tape catalogs that allow you to see what files are on what tapes? If so, how far back can you tell what information is on which tape?

Evidence Preservation Questions

- When were you instructed to preserve potentially relevant documents/data relating to the litigation?
- What actions were taken to:
- Preserve potentially relevant electronic and paper documents?
- Notify employees or third parties to stop deleting or altering potentially relevant documents/data?
- Prevent key users' PCs from being recycled should they leave the company or be given new equipment?
- Prevent key users from destroying or altering their network files?
- Prevent e-mail from being destroyed or altered?
- Prevent backup tapes from being overwritten?
- Suspend normal document destruction of offsite documents?
- What changes did you make to your tape rotation and retention policy to accommodate litigation hold requirements? When were these changes made?
- How do you determine what tapes needed to be held?
- How did you confirm you held the right tapes?

Opposing counsel will use the answers given by the IT manager or RIM manager to the foregoing questions as the foundation to support an allegation of spoliation related to a litigation matter. There is no substitute for preparation.

By: Kirke Snyder, JD, and David Isom, Esq.

SHARON HYDER, CMC, CRM ANSWERS YOUR MANAGEMENT QUESTIONS

Our organization had a major layoff last month, and another layoff is predicted. Everyone has become tense and several people are short-tempered during this crisis. Do you have any suggestions on how to handle the environment?

When times get tense, it's easy to forget the niceties. But try to avoid these behaviors that can do lasting damage.

- **SHOUTING** — Many people compound chaos by raising their voices to make themselves heard. But shouting can turn off employees and cause them to tune you out. Instead, try lowering your voice, which actually may encourage them to pay closer attention.

- **ORDERING** — Ordering. Often people under stress become abrupt and wind up sounding like drill sergeants. Remind yourself to mind your manners. Saying "please" and "thanks" will signal that you're asking, not demanding.
- **IGNORING** — When you're in crisis mode, you may push others aside. But make sure to follow up later with any employees you're brushed off and let them know that you are interested in what they have to say.

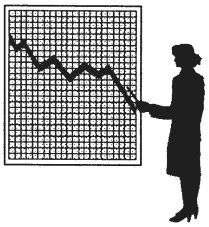
FAMOUS QUOTE

Whether you think you can or think you can't – you are right.

— Henry Ford

Trends…

Bill to Promote Health Information Technology Introduced



On February 14, representatives Ed Markey (D-Mass.) and Rahm Emanuel (D-Ill.) introduced H.R. 5442, the Technologies for Restoring Users' Security and Trust in Health Information Act (TRUST). The legislation is intended to promote the use of information technology within the healthcare system while protecting privacy and security of personal medical information.

The TRUST Act would encourage the development of health IT networks through grants and standard-setting processes while at the same time making sure that patients' medical records would be protected by setting strong privacy and security safeguards within the systems. Markey and Emanuel say the legislation empowers patients to keep their medical records out of the health IT system unless they have granted their consent, authorizes funding to enable the purchase of health IT systems, requires the use of data security safeguards (such as encryption) that make the information unreadable to individuals who are not authorized to access it, and requires patients to be notified if the system containing their health information is breached.

When introducing the bill, Markey, who is a senior member of the House Energy and Commerce Committee, said, "The spread of health IT holds tremendous promise for improving patient care, reducing medical errors, and lowering costs. But this dream could quickly turn into a nightmare for consumers without sufficient privacy and a security safeguard to protect personal medical records from unauthorized access." He also said, "With the right safeguards in place, consumers will be able to trust health IT systems, and doctors and providers will be able to confidently use this infrastructure to improve patient care."

"With the adoption of health information technology, we can reduce errors, save billions of dollars and millions of lives," said Emanuel, a senior member of the House Ways and Means Committee. "But we should never lose sight of the fact that the patient will always come first. As medical records and patient histories become electronic, phrases like 'security,' 'privacy,' and 'access' should become just as important as 'take two of these and call me in the morning.'"

Source: ARMA International Washington Policy Brief, March 2008

HYDER & ASSOCIATES
MANAGEMENT REPORT

501 W. Glenoaks Blvd., Suite 422
Glendale, CA 91202
(818) 507-0008
FAX: (818) 547-9908
E-Mail: hyder@HyderAndAssociates.com