Data Skeletons in Far-Flung Closets

October 28, 2008

Four Tips for Professionals to Prepare for Increased Regulatory and Legal Scrutiny of Electronic Communication

SEATTLE--(BUSINESS WIRE)--Oct. 28, 2008--FTI Consulting, Inc. (NYSE: FCN) - Forget haunted file rooms or ghosts roaming the halls--businesses might just find the contents of their employees' email inboxes downright terrifying this Halloween season. Every company worries about the possibility of skeletons hiding in unknown closets, but the rapid growth and proliferation of electronic stored information (ESI), especially email, has added significant complexity to the process of effectively mitigating risk.

Public exposure of private email business conversations--whether legally through court-ordered and government public information requests, or illegally through cyber hacking--has caught big-name personalities from the White House to Wall Street to Hollywood off guard. Email is the lifeblood for many organizations, and smart management of electronic communication, both by employees and company leaders, is critical to business success.

The threat of increased litigation and government regulation is also looming large because of the recent economic crisis. This is exacerbating compliance risks as electronic communications data is scattered across multiple internal and external sources, including home computers, smart phones and flash drives. Nothing is off-limits for attorneys searching for data skeletons in order to comply with legal or government discovery requests. The task of sifting through millions of electronic documents has been made exponentially easier with recent technological advances. This search through electronic files for legal evidence is called e-discovery, and new software is bringing greater speed and precision to the process.

Employees should know that their emails may be required to comply with legal or government discovery requests and that they play a central role in ensuring corporate interests are protected. Here are four tips the experts at FTI Consulting's technology practice offer about email in the workplace:

1. Do not use personal email accounts for work-related matters. This can lead to a string of legal problems, and embarrassment, as you can open up your personal correspondence to the courts, business competitors and others. If your company ends up the subject of litigation or a government investigation, IT and legal teams must examine, in a defensible fashion, nearly all of an organization's electronic communications. Some of that information will likely be presented in court or handed over to the government. If this information is located outside a company's electronic boundaries, attorneys or investigators can (and often will) have access to your personal email accounts. Companies and employees should consider enlisting experts to help develop and enforce a workplace email program that helps avoid embarrassment--and risk--for all parties.

2. Email isn't truly private and "code words" break down. No one wants to be the author of the "smoking gun" email. Today, businesses are increasingly turning to e-discovery software that incorporates advanced technologies such as data visualization and concept clustering. These technologies can quickly shine a light on euphemisms and other methods of trying to cover activities up within electronic communication. In a vivid example, a corporation recently used concept-searching software in an internal investigation of employees suspected of embezzling $50,000. A keyword search of email noted little of any value. However, using visualization and concept searching, the company was able to find an unusual number of emails between two employees using baseball terminology. Shortly after, the company was able to identify the baseball terms as code words and identify fraudulent activity totaling millions of dollars.

3. Deleted doesn't mean gone forever. The true meaning of deletion varies by company and industry under applicable regulations. Regardless, it's important to remember that hitting delete on an email or even emptying your "trash" folder doesn't mean an email is no longer discoverable. In many industries, all email is often preserved to help comply with regulations as well as the recently amended Federal Rules of Civil Procedure. Additionally, forensics specialists and investigators can help companies find and retrieve electronic data that employees may have thought that they permanently deleted.

4. Know the policy. Does your organization have an email retention and deletion policy? Now would be a good time to find out, or, as mentioned above, put one into place. Over 90 percent of organizations are actively addressing issues related to governance, risk management and compliance (GRC), yet only 9 percent of employees have a good understanding of how GRC impacts them, and only 15 percent understand their legal hold and e-discovery responsibilities, according to a survey released this month by Kahn Consulting, Inc. in association with ARMA International, BNA Digital Discovery and E-Evidence Business Trends Quarterly, and the Society of Corporate Compliance & Ethics. If you can't get answers, be proactive. Talk with your legal and IT colleagues to generate awareness and ask for additional training. This could ultimately save the company time and money as well as spare it significant risk.

"E-Discovery can be a costly nightmare if you're not prepared," said Senior Manager Director Mike Kinnaman of the FTI Consulting technology practice. Fortunately, by following the tips above, you can play a role in helping ensure your organization is prepared and minimizing its overall risk.

CONTACT: Press Only:
Edelman
Robin Bender Ginn, robin.ginn@edelman.com
Cell: 206-300-4385
Office: 206-268-2238

SOURCE: FTI Consulting, Inc.