



OCTOBER 10, 2006

IT Close Up

Building a framework for GC management of electronically stored information.

BY STEPHANIE WEINER-GIAMMARCO

IN DECEMBER 2006, proposed changes to Federal Rules of Civil Procedure—which are expected to be adopted—will require parties to discuss electronic discovery issues early; distinguish between the production of accessible versus non-accessible Electronically Stored Information (ESI); and permit parties to request the form of production for ESI. The challenges posed by ESI underscore the role of the General Counsel's Office in managing the risks of burgeoning amounts of data, diversified types of data devices and wider dissemination of both throughout an organization. Although the formalization of planning for ESI exchanges in litigation is new, general counsel offices have increasingly recognized the strategic importance of preparedness and a rapid, comprehensive response.

The practices set forth in this article are based on evaluation of effective strategies for managing ESI, as well as reverse-engineering and remedying of less successful approaches. GC offices will face different challenges based on their organizations' size, complexity, geographic scope, and industry and regulatory environments; however, all will benefit from managing ESI risk through a framework of assessing the current state of the company's Information Technology (IT) environment and ESI, and generating a plan in advance for maintenance and production of ESI.

Assessment of IT Environment

The general counsel's office needs a comprehensive understanding of the company's IT policies and procedures, organizational infrastructure and systems. An effective way to accomplish this task is to identify and appoint an "IT Liaison," an individual from the GC office who will coordinate with the company's IT department and take responsibility for comprehending the environment.

Similarly, the GC office may request that the

Stephanie Weiner-Giammarco is a director with the litigation & fraud investigation practice at BDO Seidman and leads the computer forensics, electronic discovery and data analysis practice areas. She holds certifications in public accounting and fraud investigation.

IT department identify and appoint an IT professional to be the "GC Liaison" to work with the IT Liaison. The GC Liaison typically should be an IT professional with sufficient tenure to be knowledgeable about the company's ESI and its related systems, and how they have changed, and may change, over time. The GC Liaison contributes information regarding where ESI resides, how it is stored, its backup procedures, and policy versus practice.

Through regularly scheduled meetings and ongoing communication, the IT and GC liaisons achieve a more than basic understanding of their respective departments' roles and responsibilities. Thus, the liaisons collectively understand how the company's IT environment impacts the company's legal requirements. One goal of this relationship is to generate a plan that will result in the company's effective and efficient retention and/or production of ESI in response to a discovery request or investigative need.

For the IT Liaison from the GC office, acquiring a "more than basic" understanding of the company's IT environment specifically includes an understanding of the corporate network, e-mail system, employee computer usage, the company's backup procedures, and how these have evolved over time. In addition, the education of the IT Liaison may include reviewing copies of relevant policies and procedures regarding these areas. This education facilitates the identification, retention and/or retrieval of ESI.

Initial efforts to understand the IT environment may also incorporate consideration of the potential for either user-focused discovery requests (e.g., in response to an accusation of sexual harassment) or company-focused discovery requests (e.g., in response to an accusation of financial statement fraud). Many GC offices are technologically savvy and/or have a strong sense of the ESI environment based on significant tenure as IT users in their organizations. Even experienced GC offices can benefit from asking top-level questions to generate discussion.

The following suggested questions serve to bring the GC office and IT departments together to develop a common understanding of the company's strategy for ESI. These questions are broken into four areas of the IT environment: the Network; E-mail System; Employee Usage; and Backup Procedures. Below each set of questions is a scenario that can be used as a basis for

discussion to deepen the understanding by the general counsel's office, IT department and other groups as to issues that may arise from the identification, retention and/or retrieval of ESI in response to pending or reasonably anticipated litigation or investigations.

The Network

- Do policies exist regarding the company's network use?
- How is the network organized—by group (e.g., Legal, Human Resources, etc.), by person, other?
 - Is there one server or multiple, and what does each represent?
 - What types of data are stored on the network?
 - Is each employee provided with an area on the network for his or her personal use?

Scenario: A public company is accused of materially altering its financial statements to report increased revenues. The company would like to cooperate with the Securities and Exchange Commission (SEC). In initial discussions, the general counsel's office shows a good-faith effort to assist the SEC by informing it that the individuals accused of facilitating the alleged fraud had access to personal areas on the company network, as well as certain group areas. The GC office further communicates that these areas have been identified, are in the process of being preserved, and that the company believes that the data the SEC is seeking will be covered by this preservation effort.

E-Mail System

- What e-mail system does the company use?
- Is every employee provided an e-mail account?
 - Does every employee have the ability to archive or store his or her e-mails? If so, is the default on the network or outside of the network (e.g., on the employee's desktop)?
 - Are e-mails automatically deleted after a certain period of time?
 - Is there a storage limit, and how is it implemented?

Scenario: A current employee is accused of sexually harassing a former employee six months ago through lewd and offensive e-mails. The GC

office understands the corporate e-mail structure and is aware that all e-mails are deleted from the e-mail server after 30 days, and that e-mail server backups exist for only 90 days. The GC office is also aware that every employee has a default archive located on the corporate network. In the company's initial efforts to investigate these allegations, the company identifies and preserves the e-mail archives of both the accuser and the alleged harasser.

Employees' Usage

- How and when are individuals assigned computers?
- How do employees use their computers?
- What types of data are stored on individuals' computers?
- What happens to computers when employees leave the company? Are the computers redistributed? If so, is there any "cleaning" mechanism employed prior to redistribution?
- Are these policies the same for voluntary and involuntary terminations?
- Does the company provide (or do employees use) Personal Digital Assistants (PDAs), mobile phones, or other external storage devices, such as CDs, DVDs or thumb drives?

Scenario: An employee resigned from an organization and within one month was employed by a competing business launching products that had been in the R&D phase of the former employer for the past nine months. In an initial effort to determine if the former employee should be accused of theft of trade secrets, the GC office suggested to management that it identify the former employee's laptop computer, which had not yet been reassigned, and forensically analyze it for evidence of the potential theft. That the laptop had not been reassigned was important because computer forensics professionals can obtain a bit-by-bit image of users' hard drives. The bit-by-bit image will allow for the analysis of fragments of documents, recovery of deleted files, identification of passwords for purposes of cracking password-protected or encrypted documents and other analyses.

Backup Procedures

- What are the company's backup policies and procedures?
- What data are backed up and on what media?
- What hardware/software was used to generate company backups?
- Who is the individual(s) responsible for backing up data? Discuss policy versus practice.
- Where are the backups stored (on-site, off-site or both)?
- If off-site storage, how long do the backups remain in storage? What controls are in place at the company regarding off-site storage? Is there an automatic destruction policy in place? Is there industry or regulatory guidance on an appropriate automatic destruction policy?
- How are the backup media rotated?
- What time, money and effort are needed to

retrieve data from backup media?

- Are the network and e-mail backup policies the same?

Scenario: An organization is a defendant in a breach of contract lawsuit claiming damages from 2001-2003. The general counsel's office is aware that in 2002 the company implemented a new accounting software program and that the data from prior to 2002 was transferred to the new system with very little detail. The old system is no longer supported; however, the backup tapes are still in storage because there is no automatic destruction policy in place. The organization



through ongoing communication, the IT and GC liaisons achieve a more than basic understanding of their respective departments' roles and responsibilities.

argues that the data from prior to 2002 is not readily accessible; however, the company is preserving all data in the new system in an effort to be responsive to its discovery request.

When exploring these areas, in-house counsel can also identify gaps between policy and practice by discussing these questions with IT users. Employees may be using "backup" techniques or software (such as instant messaging or customer relationship management) or purchased data sets that may not be supported by the organization's IT department.

Implementing a Plan

Once the IT and GC liaisons have a common understanding of the IT environment, the company's IT policies and procedures and the impact of the proposed changes to certain of the Federal Rules of Civil Procedure regarding discovery, they can prepare an effective, efficient discovery request response plan. The following steps are not intended to be all-inclusive, but will assist when planning to respond to future discovery requests.

- **Identify and Consult With Service Providers:** There are certain ESI-related tasks that may be more efficiently and credibly performed by independent, third-party professionals. Retaining independent, third-party professionals provides confidence that data and information have not been tampered with by company personnel and was obtained using best practices and without bias. GC offices can identify and retain service providers to perform such tasks, in addition to educating the providers about the company's IT environment. These preparatory discussions will significantly decrease response time in future litigation or investigations.
- **Develop Templates for Internal**

Communication: GC offices can also develop a plan for communication within the company. The IT and GC liaisons can formulate an efficient and practical manner to communicate document preservation requirements to the appropriate people. For example, providing draft templates to employees to test the interpretation of the directions will help mitigate uncertainty and risk of noncompliance when they are deployed in the context of a litigation or investigation. Effective employee communication based on a specific plan of action will significantly decrease the uncertainty by company employees during an investigation or request for production, thus enabling the GC office to respond more efficiently and confidently.

- **Develop Guidelines or Best Practices for IT:** Not only may employees need to preserve data in the face of litigation or an investigation, but the IT department may also need to assess the impact of any potential discovery request on its processes and procedures. Although it is impossible to anticipate every type of potential litigation or investigation, the GC and IT liaisons can develop a draft response plan and checklist of tasks, such as how to retrieve backup tapes, stop backup tape rotations or stop auto-deletion of e-mails after a certain period of time.

- **Testing the Plan:** Finally, the GC office can test the plan developed by the IT and GC liaisons. A trial run with service providers, employees and IT professionals will not only prepare all parties involved, but also reveal potential shortcomings. For example, testing a request for backup restoration may reveal that the current backup procedures are not in compliance with policy, more costly than anticipated or simply do not work. Conversely, if the tests are successful, the GC office gains comfort with the response plan.

Conclusion

The December 2006 expected-to-be-adopted changes to certain of the Federal Rules of Civil Procedure regarding discovery provide the General Counsel's Office with general guidance on the exchange of ESI. By building on historical approaches, assessing the IT environment and planning for ESI production, GC offices can manage these issues strategically. Having a plan for ESI will enable in-house counsel to advise senior management on litigation strategy, settlement options, public relations, internal investigations and regulatory inquiries based on the ability to respond quickly and thoroughly to the growing amount, complexity and distribution of data, software and devices.