The John Liner Review

THE QUARTERLY REVIEW OF ADVANCED RISK MANAGEMENT STRATEGIES

VOL. 22 NO. 3 FALL 2008

Emerging and Ongoing Issues

- **Social Trends, Risk Management, and Public Policy**
  Gerald F. Ladner
- **Emerging International Issues for Environmental Programs**
  Karl J. Russek and William P. Hazelton
- **Captives for the Middle Market**
  Don MacMeekin
- **Coverage Issues in Trade Dress Infringement Litigation**
  William J. Warfel
- **Corporate E-Mail and Electronic Documents**
  Albert Kassis
- **Mitigating the Risk of Payroll Fraud**
  Donald J. Fergus
- **Loss Development for the Non-Claims Person**
  David F. Brauer

- ISO on Enterprise Risk Management — *Supply Chain and ERM*
- Commentary — *The Myth of ERM*
- Insurance Strategies — *D&O and DIC Policy Issues*
- Insurance Law — *Military Tactics in the Courtroom*

S·P 1865
www.spcpub.com

E-mails and electronic data (electronically stored information — ESI) are now integral to litigation and investigations.

Risk Management Considerations in Regard to Corporate E-mail and Electronic Documents

ALBERT KASSIS

By now, most risk managers are aware of the issues associated with e-mails, electronic documents, databases, and records within their business environment. In legal circles and under the Federal Rules of Civil Procedure,[1] these data fall under the legal classification of "Electronically Stored Information," herein known as ESI. While these documents can be corporate assets, they also can be corporate liabilities.

This article addresses e-mail, instant messaging, e-documents, and related risks that companies face in litigation and business. Additionally, it discusses what risk avoidance strategies and undertakings should take place.

What Is Included in ESI?

ESI includes any information that is housed and can be retrieved electronically. This means documents referred to already, but also can include corporate databases, Weblogs, voicemails, text messages, and HTML files. It should be noted that it does not matter where the information is stored. This information can be on your servers, on backup tapes, or on desktops, laptops, and portable devices being used on- and off-site. Additionally, it can be content on your Web site or intranet.

The amended federal rules speed the process requiring litigants to turn over this material. The time

period has been shortened to weeks in some instances. The risk associated with over- or under-capturing data to turn over is immense. To address these issues, risk managers can undertake activities and implement policies that will reduce the risks associated with these rules and other inherent risks in the day-to-day business activity dealing with ESI.

ESI Risks Abound, From Inside and Outside

Risk managers have likely recognized risks associated with electronic intruders from the outside getting access to corporate information. While these risks are still important, there is increasing danger that comes from within the corporation. Specifically, the proliferation of electronic information may create or provide evidence of liability. The trouble is that in the day-to-day activities of a corporation, liability is lurking that may never be uncovered until ESI shows up in a legal case or investigation.

Prior to December 1, 2006, both e-mails and electronic documents were discoverable, much like paper documents; the changes that took place in the Federal Rules of Civil Procedure in December 2006 increased the level of awareness among attorneys in all practice groups. In fact, e-discovery practice groups and partners are now central in many law firms.

Prior to the federal rule changes, a number of litigating attorneys were of the "don't ask, don't tell" mentality — if one side to a legal case didn't ask for e-mails to be turned over, then opposing counsel typically would not ask either. Imagine that scenario now, particularly if a law firm or attorney loses a case. If ESI or particular ESI was never sought out and the nonrequesting side loses the case, there may be some questions to answer from both a client and a court in a potential malpractice claim.

Mishandling of ESI Risks May Cause Negative Publicity

Negative public perceptions of your entity can develop from the mishandling of ESI. This public relations risk typically arises during litigation an entity is involved in. The core legal issues in the case are typically superseded by the court focusing on one of the parties' mishandling of the ESI.

Some of the most highly publicized cases involving the mishandling of electronic discovery have become commonly known, to the detriment of the corporation involved. Most recently, legal circles are buzzing about a case simply known as the *Qualcomm* case. In *Qualcomm Inc. v. Broadcom Corp.*,[2] U.S. Magistrate Judge Barbara L. Major had sanctioned Qualcomm for "suppressing" over 40,000 electronic files. These files had been previously requested, but did not show up in discovery. As it turns out, these files were dispositive, but adversely to Qualcomm. In this scenario, Qualcomm's filing might not have taken place had these e-mails been uncovered prior to action being taken. A clear understanding of corporate e-mail policies, with policies and regimes adhered to, might have brought these e-mails to light at a juncture well before a filing took place.

The proliferation of electronic information may create or provide evidence of liability.

An equally notorious case that involved electronic data was the *Morgan Stanley* case.[3] On May 16, 2005, *The Wall Street Journal* published an article titled "How Morgan Stanley Botched a Big Case by Fumbling Emails." The merits of the matter being litigated were superseded by the negative public relations associated with the ESI issues that led to the above headlines. In both examples, the case's original legal claims took a back seat to ESI issues and how they were mishandled.

Records Retention Policies

If your company does not have a records retention policy in place now, consider instituting one as soon as feasible. Records retention policies reduce risk in many ways. A properly crafted policy provides forethought that inhibits the accumulation of structured and unstructured data that can amass. Any accumulation that does take place will be done so for a legal reason or business purpose.

Accumulation Points

All accumulating points, e.g., servers, desktop computers, and off-site locations (e.g., BlackBerries or laptops), should be addressed. We recommend that a map of where those devices are located within the

organization and who the stakeholders are for each device be developed into a living document much like an organization chart. Key members then can be assigned responsibilities to ensure that their portion of the map is kept up-to-date when changes occur. Any changes must be discussed enterprisewide, so that one department's policy does not have an impact on the policy of a different department. For example, if the research and development department (R&D) would like to keep data longer than the human resources (HR) department, both should work together to address any cross-impact.

Organizations should develop an e-mail policy with input from each and every department.

Archiving

Many corporations have adopted a basic "time and space" policy, at least for e-mail. For example, e-mails that have been created and have existed for a period of time would provoke either a deletion or archiving signal. The same would apply for data accumulation for a user. Regarding the "space" component, some employers address this issue by limiting the size of a user's "inbox." Once a threshold has been met, the user must archive e-mails, or he or she will not be able to send or receive. Practically, employees would not keep 100,000 paper documents in their office without taking action. The same should apply to electronic documents.

IT keeps data around for as long as possible, because a short-storage policy may give the appearance of deleting data to hide them. Archiving, a component of records retention, typically comes in the form of backup tapes. These tapes may retain previously deleted information and are fair game with respect to an ESI e-discovery request. The question, however, becomes whether backup tapes are "reasonably accessible" under the Federal Rules,[4] and whether a corporate litigant should be subject to the expense of searching backup tapes.

Related Issues

Related issues concern whether different departments should have different retention policies. Also, are all the interested parties communicating with each other? The information technology department (IT) typically is concerned about storage and retrieval issues. That department is not necessarily concerned about how these decisions may affect litigation that their employer may be involved in.

E-Mail Policies

Every organization needs a formal e-mail policy.

1. Organizations should develop an e-mail policy with input from each and every department. This policy will benefit the organization's counsel and will be instrumental in discovery requests.

2. Policies should include rules for retention and usage (as elaborated herein) and should be reviewed annually. Policies should be more frequently reviewed when acquisitions happen, IT systems change, or new software is implemented. Additionally, sensitive information relating to trade secrets and attorney-client work-product needs to be specifically addressed.

3. Policies need to be communicated and broadcast, with face-to-face and departmental training sessions.

4. Policies should include "instant messaging" (IM) if relevant.

   The volume of usage of IM within the work force has grown exponentially. There are risks associated with the corporation taking a passive approach towards messaging. Some corporations allow their employees to use third-party messaging services, such as Yahoo. IM that is not company-managed can create problematic log trails on corporate assets. Some of these logs can be stored on local hard drives, causing headaches for any entity trying to respond to a discovery request, while increasing risk that a trail exists unbeknown to the organization.

Litigation Hold Issues

The "Safe Harbor provision" of Federal Rules of Civil Procedure, Rule 37, safeguards an entity from charges of spoliation. This term refers to the intentional or negligent withholding, hiding, or destruction

of evidence if the entity destroys documents pursuant to a records retention policy. Specifically, 37(f) provides a safe harbor for litigants that fail to preserve ESI during normal business operations.

This rule is designed to relieve entities from sanctions for the loss or destruction of ESI as a result of routine, good-faith operations of an electronic information system. This provision allows companies to overwrite or delete older information to make way for new information. A collateral benefit is cost savings associated with the possibility of reduced storage requirements.

Preservation Letters

While the safe harbor works to offer some protection, it is limited. The records retention and destruction policy may be suspended in regard to a specific legal matter. This occurs when a company has been provided a litigation hold or "preservation" letter or notice. Such a document requires an entity to preserve ESI and disable a records retention policy currently deleting information.

When organizations are sued, generally, a preservation letter is sent from opposing counsel. It is the responsibility of the organization, upon receipt, to preserve all information defined within this letter that deals with the litigation. The preservation obligation sometimes occurs before a letter actually is presented. When the entity has reason to believe it is going to be sued, the preservation obligation arises at that time.

Implementing Litigation Holds

In both large and small organizations, preservation should not be taken lightly. From a business-operations standpoint, litigation discovery holds are intrusive. They require affirmative action. The intersection between the efforts of preserving data for this hold and the day-to-day functions of your organization needs to be addressed.

Communication Regarding a Hold

The necessity for preservation of specific data has to be communicated to all those who are related to the litigation and who control the information defined within the preservation letter. The risk is that someone may not get notice and may delete information that falls under the litigation hold.

Litigation holds apply to those working both on-site and off-site. Employees need to understand what a hold is and what their subsequent actions should be. As a measure of assurance, some organizations require affirmative hold-receipt notices whereby the employees acknowledge receipt of the hold; a log is created of all the affirmative responses. This helps to reduce risk and create a record of your efforts.

A litigation hold requires an entity to preserve ESI and disable a records retention policy currently deleting information.

Both corporations and their employees are subject to a litigation hold. While it is vital that a company understands its obligations under a hold, it is equally vital that employees do, as well. In a recent district court decision, the court imposed a $1 million fine after it concluded that spoliation took place when the company employees destroyed documents despite the corporation's efforts to preserve them in accordance with a court order.[5]

Risk managers need to work with both inside and outside counsel to assess how communications take place to implement holds. Communication regarding the hold has to be pervasive and recurring. Many corporations have established committees that deal with issues relating to preservation holds and related matters. These committees come under a number of different descriptions, including one called Discovery Action Response Team (DART). This team is made up of a cross section of individuals. Depending on the organization, it may involve counsel, IT, and department heads. Some DART teams involve various departments, including sales, R&D, and HR. DART teams are intended to develop and maintain a process and methodology for responding to ESI requests in litigation.

Locating ESI

Whether a corporation conducts a centralized or decentralized approach to preservation, information "silos" will matter.

In response to litigation or a governmental "discovery" request, entities must be able to locate and

review ESI, no matter what the format may be and regardless of language. Nuances abound that may inhibit locating this relevant information. An example would be organizational changes in software applications or versions — for instance, when a corporation switches from WordPerfect to Microsoft Word.

Many employees are not necessarily aware of the intersection of litigation and technology as it relates to electronic documents.

Additionally, a records retention policy must prohibit routine overwriting of servers and data. Special attention must be paid to servers that may "crash" and the resulting subsequent action taken, particularly if a preservation hold is in place or is expected. Also related are scenarios when new software is implemented and conversions of legacy data take place. Occasionally, with hardware upgrades, relevant data may get moved to a temporary storage device, which requires an update to any data map that the risk manager uses to monitor data silos.

Was the Hold Successful?

Ultimately, whether a preservation hold was successful or not is tested by evidentiary production to the other side. Complete document productions will result in turning over all the relevant non-privileged documents. There have been numerous instances where productions have not produced all relevant e-mails. Whether these omissions are due to inadequate production holds is not always clear. Showing a court that your organization has a well-thought-out hold strategy helps thwart any "spoliation" charge. In some states, spoliation is a separate civil action where a corporation can be held liable.

Failure to Produce ESI: Connor v. SunTrust Bank

An e-mail not showing up in production has liability impact. Take, for example, the case of *Connor v. SunTrust Bank*.[6] In that case, the plaintiff, who had adopted a child, contended that removal of direct reports to her position and changes in her job responsibilities led to the eventual elimination of her job shortly after she returned to work. An e-mail from the plaintiff's supervisor contained a statement that the position was eliminated due to the reduction from eight to three in the number of people supervised by the plaintiff. This e-mail copy was obtained by the plaintiff from a source other than the employer-defendant, who failed to produce this e-mail in responding to the plaintiff's discovery requests. The court held that plaintiff was prejudiced by the failure of SunTrust to produce the e-mail. Specifically, this failure raised the question whether all other relevant e-mail had been produced. The court additionally noted that the defendant acted in bad faith. In the court's opinion, the plaintiff's supervisor, who authored the e-mail, must have affirmatively deleted the e-mail from her sent items.

Would a properly implemented litigation hold have prevented what had occurred in the SunTrust case? Could the hold have precluded deletion? From a software standpoint, it very well could have. Beyond software, a properly educated work force could also have precluded any intentional deletion. SunTrust may never have known about the e-mail. Both inside counsel and outside counsel to SunTrust were likely unaware, because the supervisor may have been less than forthcoming and covered her tracks by deleting copies of the e-mail and not telling attorneys handling this matter.

Steps to Consider in Protecting Your Organization From ESI Risks

How would a risk manager protect a corporation from a scenario like the *SunTrust* case? There are certainly both liability issues and public relations issues associated with the *SunTrust* case.

Properly executed records-retention, e-mail, and litigation-hold policies are necessary. While properly executed policies will assist in addressing some issues, they will not stop an employee who is trying to cover his or her tracks. If the employee knows that deleting an e-mail from his or her sent box could be technologically uncovered, this knowledge might thwart the action. Indeed, many employees are not necessarily aware of the intersection of litigation and technology as it relates to electronic documents.

It is vital for risk managers to ensure that employees are aware of the following facts:

1. Deleted e-mails and ESI can be recovered.
2. Date and time of deletion can be determined.
3. Employee Internet activity can be traced.
4. Document "travel" from corporate environments to personal e-mail can be traced.
5. ESI copied to remote devices (e.g., thumbdrives) or sent to printers typically can easily be detected.
6. Voicemails potentially also could be retrieved and used for litigation.

Risk managers employed by entities that are litigious in nature and find themselves in court frequently are in an advantageous position to work with counsel to safeguard against outcomes similar to the *SunTrust* matter.

Safeguarding not only means that litigation holds are properly executed, but also that employees become more fluent in the hidden and not-so-hidden nuances of electronic documents and data. Such fluency is part of the vital knowledge needed for corporations and employees to reduce overall risk.

Have New Employees Been Schooled in the Policies of E-Mail Communication Within Your Corporation?

From an enterprise perspective, consider specific actions in regard to employees starting work at your business. New employees need to be taught the following:

1. the policies of e-mail communication between your corporation and the outside world, including business partners;
2. traps of informality in e-mail and the legacy evidentiary issues that lie therein; and
3. the binding effect of e-mail that may occur in enforcing contracts and agreements.

Corporations utilize various training and communication methods to get the message across. Some, for example, utilize their own employees to generate in-house training broadcasts. Others use podcasts that can be viewed at a user's workstation, which are ideal for those employees working remotely. These clips can be used to educate employees on mandates regarding litigation holds, e-mail policies, and inherent risks.

While e-mails may be perceived as informal in nature, they can satisfy the Statute of Frauds and create legally binding contracts.

As noted, e-mail can have a binding effect. On the one hand, while e-mails may be perceived as informal in nature, they can satisfy the Statute of Frauds and create legally binding contracts. The case of *Al-Bawaba.com Inc. v. Nstein Techs. Corp.* is an example wherein e-mail had a binding effect.[7] This case concerned a licensing agreement in which the sender had typed his name at the bottom of the e-mail. The court held that "the sender manifested his intention to authenticate the e-mail for purposes of the Statute of Frauds by typing his name, 'Denis,' at the bottom of the January 12, 2007, e-mail referencing the parties' 'contractual agreement'."

So, even though the informality of e-mail may be relied upon merely to facilitate communication, a possible unintended result may be that an employee is able to bind a corporation in a contract merely by e-mail. Additionally, the binding effect of e-mails can also have an impact in the personal affairs of those employees that use work e-mail to conduct personal business. The implication is that any future enforcement of agreements or contracts can subject data on the employer's network to discovery requests because of the binding effect of e-mail.

ESI Corporate Policies Should Be Communicated and Reinforced

Regarding new and existing employees, you should be able to affirmatively answer the following questions.

1. Does your orientation program address

employees' use of corporate systems and e-mail-use policies?

2. Are there training programs in place that address these issues for the continuing work force?

3. Is there an "Acceptable ESI Use Policy" drafted, disseminated, and communicated?

4. Are employees educated on the ramifications that e-mails can have on creating a binding contract, providing proof in litigation, and, generally, on creating liability?

Imagine the overall benefits of creating, fostering, and educating employees as to the above policies. Specific examples such as the scenario that played out in the *SunTrust* case above should be communicated. An employer's proactive approach will inhibit risk along many fronts.

Personnel- and Employment-Related ESI Risks

Use of e-mails as evidence in litigation is more common in legal actions related to personnel and employment matters. E-mails have a unique impact on employee-related claims against an employer or manager.

Almost three-quarters of all litigation against corporations is employee-related.[8] From a risk standpoint, employment-related litigation is different from other forms, since the plaintiff-employee is actually part of the work force. The communications between all the parties are embodied within the e-mail and electronic document environment of the employer and can easily be moved to a third-party e-mail or printed as evidence that the communication happened. As noted, in *Connor v. SunTrust Bank*, the employee had copies of the e-mail in hand, which made it more difficult for the employer to prove that none existed.

In *Zubalake v. UBS Warburg LLC*, the plaintiff, Laura Zubalake, had copies of pertinent e-mails in hand. When those e-mails were not part of the production set, the judge ordered backup tapes searched.[9] In a number of these matters, judges appear to impose a more stringent discovery requirement because the data are under the employer's control.

Exit Interviews as a Mechanism in Reducing Risk

Exit interviews are always important to employers. They offer many advantages, including insight on employees' attitudes toward their former positions, toward supervisors, and toward the general corporate environment. Equally important is to gauge whether an exiting employee intends to take legal action after leaving employment. Employers take various actions regarding data and e-mails previously within the exiting employee's control. For example, employers often "wipe" hard drives of exiting employees, resulting in lost data. It is always best to wait to take action of this nature. An alternative would be to make a mirror copy or image of the hard drive if it is possible that the exiting employee will pursue litigation.

ESI as an Investigatory Asset

Companies are subjected to a multitude of regulatory burdens. Consider the utilization of e-mails or e-documents in investigations as a mechanism to reduce risk. HR or legal counsel can search an employee's e-footprint to investigate issues relating to the following:

1. violations of HR rules and policies, such as sending of sexually oriented e-mails;
2. conduct in violation of Sarbanes-Oxley;
3. violations of the Foreign Corrupt Practices Act;
4. issues involving the Securities and Exchange Commission;
5. trade secret misappropriation; and
6. various state and federal regulations.

Consider that on a regular basis, many high-profile individuals find themselves at the center of attention because of e-mail communication. Consider founder Bill Gates' e-mails, introduced in support of the government's antitrust case against Microsoft.[10] More recently, two hedge fund managers for Bear Stearns were taken into custody over roles they had in the collapse of their hedge funds. Ralph Cioffi and Matthew Tannin are facing criminal charges because Tannin allegedly said in an e-mail that he was "afraid that the market for bond securities they

had invested in was 'toast.'" According to *Bloomberg News*, he suggested shutting the funds. Several days later, though, the two managers told investors that they were comfortable in holding their funds.[11]

The term "smoking gun" is used for e-mails that are clearly damaging to an entity or individual. Because e-mail is treated much like chatting, often treated as private and unofficial, it is very susceptible to misinterpretation. A properly executed collection of ESI policies and procedures, continually reinforced, would go a long way toward averting risk.

In May 2008, Forrester Research, along with an e-mail security company, released a survey of more than 300 U.S. companies.[12] The findings dealt with outbound security and e-mail. The survey came up with the following findings:

- 34 percent of the companies surveyed had had e-mails subpoenaed in the past year;
- 26 percent of the companies had terminated employees for violations in e-mail policies;
- 27 percent of the companies had investigated a leak in sensitive information via a lost or stolen mobile device; and
- 41 percent of the large companies with more than 20,000 employees employ staff to monitor e-mail.

The results are eye-opening, at the least. Consider the prospect that these percentages will only get higher, given proliferation of these requests as permitted by the Federal Rules of Civil Procedure and the soon-to-be-majority of states that have adopted rules that emulate the federal rules.

Proactive Data Mining

Using ESI as an investigatory asset should be a precursor to engaging in litigation. Many organizations are now hedging risk by mining data on their own servers prior to filing a lawsuit. This allows discovery, prior to filing, of any unforeseen scenarios where smoking guns that may hinder a lawsuit exist.

Advanced technology and software allow companies to automatically detect violations of e-mail policy. This technology can sequester risky e-mails for the purpose of limiting liability. Most implementations of this type of software involve establishing "acceptable use" policies. Some policies include key words that are banned. These words are then programmed into the lexicon of the software that scans e-mail messages. Some software allows for multiple lexicons for different business units. Some applications prevent mass e-mails that may be used in marketing and may require disclaimers in certain industries. Software can also be used to prevent use of e-mail within certain departments of a company. This would potentially prevent theft of trade secrets or other information.

A properly executed collection of ESI policies and procedures, continually reinforced, would go a long way toward averting risk.

Messagegate Inc. has conducted studies of the uses of e-mail. In one such study, involving several sample e-mails and violations of acceptable use, the violations are worth noting.

- Users misaddress e-mails, leaking sensitive data.
- Employees bypass corporate security measures by sending documents to personal Web-based e-mail accounts.
- Social Security numbers were included in some e-mails.
- Offensive e-mails are commonly sent within the enterprise.[13]

Inherent Risk of Metadata Within ESI

"Metadata" is defined as data about data. It is vital to ensure that your organization is aware of the risks associated with metadata.

Documents leaving a corporate environment in their native applications can pose major risks. Microsoft's Word software has the ability to capture data behind the scenes that can create substantial risks. Specifically, the metadata captured and associated

with a Word document can reveal the original author and the date of the document's creation. Additionally, if a document is being drafted and a tool known as "track changes" is being used, all the revisions and comments between the parties are tracked and can be uncovered if the document remains in its native form when given to a third party.

Documents leaving a corporate environment in their native applications can pose major risks.

Consider some ramifications. Individuals, who may be customers or even competitors, receiving the document can utilize their own software's "track changes" tool to see what the sending party's changes were. They can also see if the sender was actually the creator of the document. They can also determine if an agreement was drafted for a different entity, potentially identifying your company's other clients. They may gain advantage by seeing terms negotiated for other clients that are not part of the terms of the agreement within their hands. Private and confidential information may be made public.

Two publicized metadata snafus follow.

1. During the nomination process of Judge Samuel A. Alito to the Supreme Court, the Democratic National Committee put out a memorandum criticizing his nomination. This document was disseminated in its native form. It was later discovered through the metadata that the document was written well before the judge's nomination.[14]

2. An announcement by the law firm Bois Schiller regarding a lawsuit revealed through the metadata a potential future defendant whose identity the firm wanted to keep private.[15]

Many corporations require that documents leaving an electronic environment within the organization do so in a static or petrified "image format." For the most part, Adobe's PDF format accomplishes this.

Risks of Human Error

Other ESI risks may come about by human error. Some e-mail software has an "auto look up" or "auto-fill" feature that allows frequently used e-mail addresses to be inserted within an e-mail "send line." Consider a recent scenario involving an Eli Lilly in-house attorney who was working on a very large settlement. After drafting an e-mail full of company-sensitive information, which included information on a fine to be paid, the in-house attorney inadvertently sent the e-mail to a *New York Times* reporter instead of outside counsel. The reporter had a similar last name to outside counsel. The auto-fill e-mail feature in the e-mail software facilitated an inadvertent submittal. News of the e-mail became widespread soon thereafter.[16]

Strategies With Service Partners Help Reduce Risk

In years past, when corporations were involved in litigation, they typically looked at their outside counsel to make decisions on which service partners to use to support the efforts of counsel. Risks were minimal because information, particularly electronic data, was confined and not of the same significance as today. Currently, the environment is changing, in that corporations are formalizing internally what service partners to use and are imposing those decisions on outside counsel. Service partners are of critical importance. A particular decision on a service partner can increase or decrease the risks associated with ESI. Equally important are the costs associated with the service-partner decisions.

There are a number of risk-reduction benefits in choosing service partners internally.

- Corporations are establishing formal requests for proposals (RFP) for service partners, tailored toward their specific needs, architecture, and workflow.

- Inside and outside counsel are collaborating to establish RFP requirements that produce overall efficiencies.

- Workflows are recognized. Selected service providers understand their clients and maximize that

knowledge to handle ESI.

- Service providers can establish business practices that conform to the corporate client's requirements, including specific billing procedures.
- Down time associated with training and interacting with law-firm-selected service partners is kept at a minimum.
- Legal technology can be coordinated more appropriately with the corporation's IT staff, resulting in efficiencies and other benefits to a number of departments.
- ESI technologies associated with flagging and indexing work product and those associated with privileged ESI can be integrated, resulting in less risk of documents being released in a litigation production despite counsel's technological protections that would prevent such release.

ESI Solutions for Enterprise E-Discovery

While selecting service partners is beneficial, it may not make total sense all the time. Some companies and industries are more subject than others to all the issues described in this article. If the issues raised are routine and part of the day-to-day corporate existence of the corporation, risk managers possibly need to seek out enterprise solutions for many of these issues. Now is the time to consider making such a move, since data are growing at an exponential rate. While outsourcing some of these tasks, such as ESI collection, review, and monitoring, makes sense in organizations with infrequent litigation, it doesn't with those entities in court on a weekly basis. The software that prevents use of e-mail by certain departments, referred to above, provides one component of the enterprise solution. Other applications provide other components of the solution.

- Litigation hold software isolates relevant custodial data for preservation purposes.
- Data architecture software maps and updates data silos and stakeholders.
- Certain software isolates, collects, and harvests globally across an enterprise's data pursuant to a discovery request.
- Evidence-review applications streamline review of data.

Insurers are taking a hard look at coverage for discovery costs associated with ESI.

Corporate Insurance Implications

Insurers are taking a hard look at coverage for discovery costs associated with ESI. Several insurers have generated specific electronic discovery insurance coverage that provides some degree of protection against discovery costs. Some insurers that offer coverage are mandating training programs or requiring exclusions.

There are ancillary benefits to purchasing this coverage. In conjunction with writing a policy, typically, the insurer audits the ESI structure, which assists risk managers in uncovering weaknesses and addressing shortcomings. Chubb Group, for example, has issued publications and advice on records management and issues relating to ESI.[17] Insurers are in a unique position to oversee this process, in that they are commonly both litigant and underwriter. In that regard, they likely will be a resource for best practices for some time to come.

Conclusion

At times, the proliferation of electronic data and the current habits of the work force collide, creating increases in risk. In regard to ESI, risk managers perform a similar role to that of safety officers. Best practices must be communicated and their use monitored; perpetrators must be sanctioned if violations occur. The business community has recognized ESI risk. Technologies are being developed to help increase management of ESI and curb activity that would be adverse to ESI management. The education, monitoring, and continual reinforcement of ESI policies will lead to an enterprisewide decrease in risk.

Endnotes

1. See Cornell Web site for E-Discovery, http://www.law.cornell.edu/rules/frcp/index.html.
2. *Qualcomm Inc. v. Broadcom Corp.*, Case No. 05cv1958-B (BLM) (S.D. Calif., Jan. 7, 2008).
3. *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, 2005 WL 679071 (Fla. Cir. Ct., March 1, 2005).
4. See FRCP Rule 26(b)(2)(B), Duty to Disclose: General Provisions Governing Discovery, http://www.law.cornell.edu/rules/frcp/Rule26.htm.
5. See *In re Prudential Insurance Company of America Sales Practice Litigation*, 169 F.R.D. 598 (D.N.J., 1997).
6. *Connor v. SunTrust Bank*, 2008 U.S. Dist. LEXIS 16917 (N.D. Ga., March 5, 2008).
7. *Al-Bawaba.com Inc. v. Nstein Techs. Corp.*, No. 45550/07, 2008 N.Y. Slip Op. 50853(U), 2008 WL 1869751 (Sup. Ct. Kings Co., April 25, 2008).
8. See Equal Employment Opportunity Commission Web site, www.eeoc.gov.
9. *Zubulake v. UBS Warburg LLC*, 231 F.R.D. 159 (S.D.N.Y., 2005).
10. Wikipedia, "United States Microsoft antitrust case" (last modified August 8, 2008), available at http://en.wikipedia.org/wiki/United_States_v._Microsoft.
11. Hurtado, Patricia, and Thom Weidlich, "Ex-Bear Stearns Fund Managers Indicted for Fraud (Update 4)," Bloomberg.com (June 19, 2008), available at http://www.bloomberg.com/apps/news?pid=20601087&refer=home&sid=aefVn_KahdBI.
12. "Outbound Email and Data Loss Prevention in Today's Enterprise, 2008," Proofpoint (May 2008), available at http://www.proofpoint.com/id/outbound/index.php.
13. Bradley, Chris, "Unintentional Employee Misuse Top Driver for Enterprise E-Mail Risk," CUNA Technology Council (July 28, 2008), available at http://www.cunatechnologycouncil.org/news/2242.html.
14. Zeller, Tom, "Beware Your Trail of Digital Fingerprints," *The New York Times* (November 7, 2005), available at http://www.nytimes.com/2005/11/07/business/07link.html?ei=5090&en=98e8af679a0797f4&ex=1289019600&partner=rssuserland&emc=rss&pagewanted=print.
15. Wagner, Jim, "Scrubbing Content Metadata," internetnews.com (August 23, 2004), available at http://www.internetnews.com/ent-news/article.php/3398651.
16. Eban, Katherine, "Lilly's $1 Billion E-Mailstrom," Conde Nast Portfolio.com (February 5, 2008), available at http://www.portfolio.com/news-markets/top-5/2008/02/05/Eli-Lilly-E-Mail-to-New-York-Times.
17. "Loss Prevention Resources," The Chubb Group of Insurance Companies, available at www.chubb.com/businesses/chubb3331.html.

Albert Kassis is an attorney and CPA