Carnegie Mellon CyLab
CONFIDENCE FOR A NETWORKED WORLD

INTERNET SECURITY ALLIANCE

MARCH 2007 VOL. 1 NO. 2

E-DISCOVERY RISK MANAGEMENT

ENTERPRISE RISK INTEGRATION PROGRAM: PERSPECTIVE

Carnegie Mellon University
CyLab

AUTHOR

Jody R. Westby

Table of Contents

ENTERPRISE RISK INTEGRATION PROGRAM: PERSPECTIVE

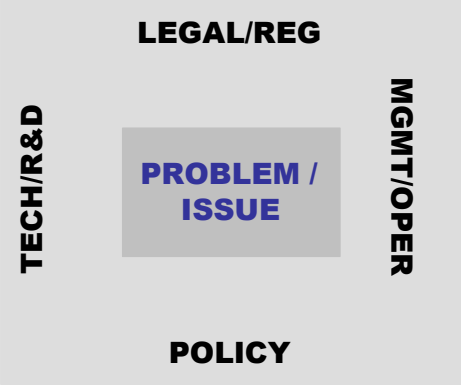
By Jody R. Westby[1]

BACKGROUND ON ENTERPRISE RISK PERSPECTIVES

Carnegie Mellon CyLab, in collaboration with the Internet Security Alliance (ISAlliance), has created an Enterprise Risk Integration Program to examine specific risk issues from a multidisciplinary perspective, taking into account legal, technical, operational/managerial, and policy considerations. Quarterly Perspectives are distributed to CyLab and ISAlliance corporate members and are posted in the Enterprise Risk Integration Repository on the members-only section of the CyLab Web site (www.cylab.cmu.edu).

The Perspectives are designed for a multidisciplinary audience and should be shared with the appropriate personnel within CyLab and ISAlliance member organizations to help foster a coordinated approach to cyber security, privacy, and risk management issues. At a minimum, the Perspectives are suited for general counsels (GC), chief information officers (CIO), chief information security officers (CISO) or chief security officers (CSO), chief technology officers (CTO), chief executive officers (CEO), and senior management. A series of CyLab teleconferences follow each Perspective to enable members to delve more deeply into the topic area and enhance their understanding of the covered risks.

E-Discovery Risk Perspective



This Perspective focuses on the amendments to the Federal Rules of Civil Procedure (FRCP or Rules) that became effective December 1, 2006. The new Rules specifically allow the discovery of electronically stored information (ESI) and impact how litigation is managed. CyLab teleconferences scheduled around the E-Discovery Risk Management Perspective are a four-part series to be held on:

March 8: Data Preservation and Sanctions: The Alligator in the Swamp in Alive and Well

March 15: What Data is "Not Reasonably Accessible?"

March 22: Technical Discovery Tools: Snake Oil or Silver Bullets?

March 29: Managing E-Discovery: Security and Governance

[1] Jody R. Westby, Esq. serves as Adjunct Distinguished Fellow for CyLab and is CEO of Global Cyber Risk LLC. She chairs the American Bar Association's Privacy & Computer Crime Committee and is the editor and co-author of four books on privacy, security, cybercrime, and the development of enterprise security programs.

Considerations

These programs will be archived by program date on the CyLab Web site and can be viewed at any time by personnel from CyLab or ISAlliance member organizations. If there is interest in pursuing one or more aspects of e-discovery risks in greater detail, please notify Jody Westby, CyLab Adjunct Distinguished Fellow, at jwestby@andrew.cmu.edu. We welcome your input on topics and programs.

E-DISCOVERY RISK MANAGEMENT

Legal issues are customarily driven by managerial, operational, or policy factors rather than technological considerations. The amendments to the FRCP, which specifically allow electronic discovery, went into effect December 1, 2006, and changed that long-standing paradigm.[2] *Technological considerations are now front and center in litigation strategy, and discovery issues must be woven into enterprise security programs.* Although the amended Rules were six years in the making, general counsels and information security personnel have been caught off-guard. An October 2006 survey of corporate counsel conducted by LexisNexis revealed that only seven percent of corporate attorneys were prepared to meet the requirements of the new Rules.[3] Moreover, in most organizations, the interaction between legal counsel and technical security personnel is limited, making the integration of e-discovery requirements into security programs more difficult. *Today, proper management of litigation risks requires an understanding of the interdependencies between the various legal, operational, policy, and technical considerations involved in complying with the new FRCP.*

► THE LEGAL & REGULATORY PERSPECTIVE

The changes to the FRCP are based on the notion of discovery containment and judicial supervision. Understanding that digital discovery can easily involve massive amounts of data, the Rules aim to strike a balance between which data is relevant and accessible, and which is not. They were not drafted with the intent that they be used by litigants to seek vast amounts of digital data, such as full images of servers and disc drives. Rather, the amended Rules are intended to rein in discovery and confine it to what is specifically relevant to the matter at hand. Toward this end, judges may be better prepared for the new Rules than counsel. The National Judicial College has been developing training courses and materials to bring judges up to speed on the FRCP amendments and help them understand issues surrounding electronic discovery. Thus, many judges may refuse to accept the old, generalized arguments about burden and expense associated with the discovery of electronically stored information (ESI). Ken Withers, senior judicial attorney of the Federal Judicial Center notes that:

---

[2] *Amendments to the Federal Rules of Civil Procedure,* U.S. Supreme Court, Apr. 12, 2006, http://www.supremecourtus.gov/orders/courtorders/frcv06p.pdf.

[3] "Survey: Only 7% of Corporate Counsel Attorneys Rate Their Companies Prepared for New Federal Rules on Electronic Discovery," LexisNexis Press Release, Nov. 28, 2006, http://www.lexisnexis.com/about/releases/0940.asp.

No attorney can go into a federal court today and try to bluff their [sic] way through an e-discovery case. That will no longer work. If you say e-discovery is burdensome, the judge will expect plenty of detail as to why it's such a burden. And if you're the requesting party, you'd better be able to explain exactly what needs to be produced and why it is important.[4]

In addition to requiring attorneys to have solid explanations regarding the ESI they are seeking or trying to prevent from being discovered, the new Rules also change the interaction between counsel and impact litigation strategy. Whereas discovery used to be addressed after motions and pre-trial negotiations, the amended FRCP require the parties to know what ESI they have almost from the start of the case and to meet and "confer" no later than the 99th day after the matter was filed to work out a discovery plan. This requirement significantly impacts how the attorneys interact and the strategy of the case is shifted from motions to initial discovery and the costs of producing ESI.

A SUMMARY OF THE RULE CHANGES

The changes to the FRCP are straightforward and apply to Rules 16, 26, 33, 34, 37, 45 and Form 35.

Rule 16: Pretrial Conferences/ Scheduling; Management

The amendment to Rule 16 includes ESI as one of the topics that may be included in a pretrial scheduling order. The order may also include any agreements the parties have reached regarding claims of privilege or protection of trial-preparation material. This amendment is intended to alert the court to address discovery of ESI early on in the case and to minimize the risk of disclosure of protected information.

Rule 26: General Provisions Governing Discovery: Duty of Disclosure

The amendments to Rule 26 have the greatest impact on litigation strategy and how e-discovery is to be handled.

- Rule 26(a) directs a party to provide "a copy of, or a description by category and location of, all documents, electronically stored information, and tangible things that are in the possession, custody, and control of the party." This "description and location" document must be provided to the other party without waiting for a discovery request. It is one of the most important requirements of the amended Rules and is certain to have a significant impact on litigation strategy.

- Rule 26(b)(2)(B) states that ESI which a party identifies as "not reasonably accessible because of undue burden or cost" need not be produced. Even if the party who makes this claim successfully meets this burden, the court may still order such discovery if the other party shows good cause.

[4] Scott Gawlicki, "E-Discovery Grows Up," *Inside Counsel,* Feb. 2005, http://www.insidecounsel.com/issues/insidecounsel/15_159/features/186-1.html.

According to the Judicial Conference of the United States, examples of data that may be considered "not reasonably accessible" (NRA) could include:

- backup tapes that are not indexed, organized or conducive to electronic searches;
- legacy data that was created by obsolete systems; and
- data that has been "deleted" but is still in fragmented form.

- In the context of the amendments, it is important to note that Rule 26(b)(2)(C) allows a court to limit discovery, including ESI, if it determines that:
  - the discovery is unreasonably cumulative or duplicative;
  - the information can be obtained from another source that is more convenient; or
  - the burden or expense of the production outweighs its likely benefits.

  The Civil Rule Advisory Committee Notes (CRAC Notes) accompanying the e-discovery amendments state that the decision on whether to require a party to search for and produce data that is NRA depends on whether the burdens and costs can be justified in the circumstances of the case. The CRAC Notes indicate that appropriate considerations include (1) the specificity of the request, (2) the quantity of information available from more accessible sources, (3) the failure to produce information when it existed in a more accessible form, (4) the likelihood of finding relevant, responsive information that could not be found in more accessible sources, (5) the predictions as to the usefulness or importance of the data, (6) the importance of the issues at stake, and (7) the parties' resources.

"In addition to requiring attorneys to have solid explanations regarding the ESI they are seeking or trying to prevent from being discovered, the new Rules also change the interaction between counsel and impact litigation strategy."

- Rule 26(b)(5) protects privileged or protected trial preparation materials that are inadvertently produced in discovery. The CRAC Notes explain that the risk of waiver from producing privileged or protected materials increases substantially because of the volume of ESI and the difficulty of reviewing it. The amendment enables the disclosing party to notify the other party of a claim of privilege or protection and the basis for the claim, and it requires the receiving party to promptly return, sequester, or destroy the information. The other party is also prohibited from using or disclosing the information until any dispute about it is resolved. The amended rule recognizes the inherent risk of waiving privilege or protections afforded to trial preparation materials in the electronic environment and the substantially higher costs of reviewing ESI to ensure such data is not produced. This amended rule is intended to facilitate e-discovery by providing a "claw back" provision for privileged and protected information in the event this occurs.

- Rule 26(f) requires parties to meet and "confer" on the discovery of ESI "as soon as practicable" but not less than 21 days before a scheduling conference is held (the parties need to meet by the 99th day after the case is filed) . The amended rule requires the parties to develop a discovery plan (pursuant to Form 35 – Report on Parties' Planning Meeting) that addresses:
    - relevant and accessible ESI;
    - the form in which the ESI is to be produced;
    - issues regarding privilege or protection; and
    - what ESI should be subject to preservation.

  As noted earlier, this amendment significantly moves discovery up on the litigation timeline and impacts litigation strategy.

Rule 33: Interrogatories to Parties

The amendments to Rule 33 simply allow a party to answer an interrogatory question by referring to ESI where the answer may be derived or ascertained.

Rule 34: Production of Documents, Electronically Stored Information, and Things and Entry Upon Land for Inspection and Other Purposes

The amendments to Rule 34 allow a party to request that they be able to "inspect, copy, test, or sample any designated documents or electronically stored information (including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium…)" or to inspect "tangible things that constitute or contain matters within the scope of" discovery. This amended rule also allows the requesting party to specify the form in which ESI is to be produced. The responding party may object to the form in which the ESI is to be produced and specify the form it intends to use. If the requesting party does not specify the form in which ESI is to be produced, the responding party must produce the information in the form in which is it ordinarily maintained, or in a form that is reasonably usable.

The CRAC Notes confirm the importance of this Rule by declaring that, "Rule 34(a) is amended to confirm that discovery of electronically stored information stands on equal footing with discovery of paper documents." The CRAC Notes also clarify that parties may request the opportunity to test or sample ESI or inspect another party's electronic information system, but the Notes caution courts to "guard against undue intrusiveness resulting from inspecting or testing such systems."

Rule 37: Failure to Make Disclosures or Cooperate in Discovery: Sanctions

The amendments added a new subparagraph to Rule 37 which recognizes the reality that the ordinary use of electronic systems involves the routine alteration and deletion of data. Rule 37(f) creates a "safe harbor" and specifies that a court may not impose sanctions for failing to produce ESI that was lost as a result of the "routine, good-faith operation of an electronic information system." The CRAC Notes, however, explicitly state that the "good-faith operation" of systems requires parties to modify or suspend routine features of a system that may result in the destruction of data that is subject to preservation. A party is under a duty to preserve data that is applicable to pending or reasonably anticipated litigation.

Rule 45: Subpoenas

Rule 45 allows subpoenas to include ESI, including the testing, sampling, copying, and inspection of ESI.

PRACTICAL IMPACT OF FRCP E-DISCOVERY AMENDMENTS

The practical impact of the e-discovery amendments to the FRCP is that attorneys must rethink how they manage discovery and move away from the traditional notion of boxes of paper documents and traditional filing systems. Today, almost all corporate data is digital. It may be kept in multiple information technology (IT) systems, stored in a variety of formats, kept in different locations, and be subject to varying backup and retention policies.

From the moment litigation is filed or a person has reason to believe litigation may arise, counsel must know:

- What ESI the organization has
- What ESI is relevant
- What ESI should be preserved
- What ESI is subject to privilege or other protections (including intellectual property protections, contractual obligations, non-disclosure agreements, etc.)
- What format is the ESI ordinarily maintained in
- Where the ESI is located and how many copies exist
- What personnel have access to the ESI (within the company and third parties, such as vendors, contractors, business partners, etc.)
- What ESI is not reasonably accessible
- What ESI is expensive and burdensome to produce.

Counsel who has a firm grasp on this information will have a decided advantage over counsel who does not. They will be able to:

- Quickly determine what is relevant and discoverable;

- Produce the required "description and location" document in the timeframe required by Rule 26;
- Narrowly determine what data is relevant, thereby significantly narrowing the scope of discovery, avoiding overproduction of data, and reducing the chance of producing privileged or protected data;
- Better meet their burden of proof in resisting discovery of data that is privileged, protected, or NRA;
- Cut discovery costs by saving time in locating relevant data, reducing disruptions to business, and producing data in electronic format versus paper;
- Mount a strong challenge to requests seeking to test or sample ESI or inspect IT systems – something no party wants granted.

In addition, when one party is obviously knowledgeable about its data and systems and the opposing side is not, it may be easier to convince the court that access to the opposing side's IT systems or data should be granted or that large amounts of electronic data should be produced.

"The CRAC Notes, …explicitly state that the "good-faith operation" of systems requires parties to modify or suspend routine features of a system that may result in the destruction of data that is subject to preservation."

SCOPE OF E-DISCOVERY AMENDMENTS

The Rules specify that ESI includes "writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium,." The CRAC Notes refer to the "broad meaning" of ESI in Rules 26(a)(1)(B) and 34(a). Prior to the amended rules going into effect, however, many cases have involved ESI and courts have had to address what electronic data would be discoverable. In *Vioxx Products Liability Litigation,* No. MDL 1657, (E.D.La. Feb. 18, 2005), for example, the court found that "'documents, data and tangible things' is to be interpreted broadly to include…electronic messages, voice mail, E-mail, telephone message records or logs, computer and network activity logs, hard drives, backup data, removable computer storage media such as tapes, discs and cards, printouts, document image files, Web pages, databases, etc." Thus, it is reasonable to conclude that ESI would encompass email, text messages, instant messages, voice mail, content and images on cell phones, Blackberries, and other personal digital assistant devices, thumb drives and other external storage devices, and web-based applications and data. Voice Over Internet Protocol networks carrying both data and voice are also vulnerable to discovery.[5]

[5] *See, e.g.,* David Sumner and Damon Reissman, "E-Discovery May Target Unexpected Sources," *E-Commerce Law & Strategy,* Dec. 4, 2006, http://www.law.com/jsp/legaltechnology/PubArticleFriendlyLT.jsp?id=1164981804524; Rebecca Herold, "Finding Data Needles in Electronic Haystacks," *Computer Security Alert,* Computer Security Institute, Nov. 2006 at 8-10.

Although the FRCP apply only to federal cases, they are already impacting state court rules of evidence. The National Conference of Commissioners on Uniform State Laws (NCCUSL) is currently working on draft Uniform Rules Relating to the Discovery of Electronically-Stored Information. The NCCUSL Drafting Committee concluded early on that the significant issues relating to e-discovery had already been dealt with in the six years leading up to the amendments to the FRCP. In its November 2006 draft, the NCCUSL Drafting Committee specifically noted that:

Accordingly, this draft mirrors the spirit and direction of the recently adopted amendments to the Federal Rules of Civil Procedure. The Drafting Committee has freely adopted, often verbatim, language from both the Federal Rules and comments that it deemed valuable. The rules are modified, where necessary, to accommodate the varying state procedures and are presented in a form that permits their adoption as a discrete set of rules applicable to the discovery of electronically-stored information.[6]

THE POLICY PERSPECTIVE

Policy pressures on e-discovery are coming from the International Organization for Standardization (ISO), Rules of Professional Conduct for attorneys, and EU privacy authorities.

ESI raises significant authenticity and data integrity issues. The public's level of awareness regarding the ability to alter or manipulate digital data has been raised significantly in the past couple of years, largely due to several well-publicized instances involving manipulated photographs.[7] Therefore, attorneys are much more likely to question digital evidence and seek proof that the data produced is the original information (authenticity) and that it has not been tampered with or altered in any way (integrity). In seeking common ground in addressing such issues, it is likely that courts and counsel alike will turn to established best practices and standards.

ISO standard15801, adopted in 2004, pertains to the trustworthiness and reliability of information stored electronically.[8] The standard references the operation of IT systems and where issues of trustworthiness, reliability, authenticity, and integrity of stored information are important. It does not cover processes used to evaluate the authenticity of information prior to it being stored in the system, but it can be used to demonstrate that

[6] *Uniform Rules Relating to the Discovery of Electronically-Stored Information,* National Conference of Commissioners on Uniform State Laws, November 2006 Drafting Committee Meeting, Dec. 6, 2006 at 4, http://www.law.upenn.edu/bll/ulc/udoera/2006postdraftnovember.htm.
[7] "Digital Tampering in the Media. Politics and Law," Dartmouth University, http://www.cs.dartmouth.edu/farid/research/digitaltampering/.
[8] ISO/TR 15801:2004, "Electronic Imaging – Information stored electronically – Recommendations for trustworthiness and reliability," International Organization for Standardization, 2004, http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=29093.

the output from the system is a true reproduction of the original document.[9] Many companies may try to integrate ISO 15801 into their information security program to enhance their ability to address authenticity and integrity issues.

Metadata, or "data about data," is another area that has policy implications. Word documents have "properties" that indicate who worked on the document, the dates and times it was created, modified, or printed. This metadata can reveal valuable information to persons who are non-clients. Therefore, counsel should take care to remove metadata from word processing files before they are circulated to non-clients. This can be done by running the document through "scrubbing" software or sending it in pdf format using Adobe Acrobat software. The American Bar Association (ABA) and New York Committee on Professional Ethics have each ruled that an attorney's failure to remove or block metadata violates their professional codes of conduct (the Model Rules of Professional Conduct (Model Rules) for the ABA and the New York Disciplinary Rules) regarding the duty to safeguard client confidences. Once metadata is released, however, it is usable by the opposing side. The ABA ruled in Formal Opinion 06-442 that the Model Rules did not prohibit a receiving attorney from reviewing or using confidential information contained in metadata.[10] These rulings raise several questions:

"Therefore, counsel should take care to remove metadata from word processing files before they are circulated to non-clients."

- Should metadata be removed from discovery data?
- If metadata is scrubbed from discovery data, could that be deemed to be destruction of evidence?
- If documents are produced in pdf format, could that be interpreted as withholding relevant information?
- Could an attorney be subject to disciplinary action for producing metadata embedded in ESI?

Absent clear authority on this issue, counsel should research rulings in their jurisdiction and seek clarification with opposing counsel or the court.

Outsourcing and distributed global operations make it all the more likely that the FRCP Rules will have a significant impact on multinational corporations. Companies with offices or parent corporations located in the U.S. are likely to be asked to produce ESI relevant to litigation matters. Requests for ESI discovery or subpoenas to produce ESI can be served on U.S. entities and may call for the production of electronic data held in foreign locations. Absent

[9] *Id.*
[10] "Editorial: Preventing Metadata Disclosure," *New Jersey Law Journal,* Nov. 29, 2006, http://www.law.com/jsp/legaltechnology/PubArticleFriendlyLT.jsp?id=1164725055936.

consent (which would be rare), potential legal issues arise when parties send personally identifiable information (PII) protected under the EU Data Protection Directive across borders to entities that are not in a jurisdiction deemed to provide "adequate" privacy protections or the receiving entity does not participate in the U.S. Safe Harbor program.[11] Although Article 26 of the Directive allows transfers of personal data "for the establishment, exercise, or defence of legal claims," this Article has been interpreted very narrowly by European data protection authorities.[12] Accordingly, if EU authorities were to begin blocking transborder discovery of data and impeding litigation, the U.S. government would surely inject itself and try to negotiate a resolution. In the meantime, companies should cautiously examine cross-border discovery and seek clarification from national data protection authorities when it seems prudent to do so.

► THE MANAGERIAL & OPERATIONAL PERSPECTIVE

The amended Rules are having a significant impact on managerial policies and procedures and operational considerations. Organizationally, they require a much closer working relationship between in-house counsel, the CISO, and records management personnel. Operationally, they require a linkage between records management systems and enterprise security programs.

The average American company deals with 305 litigation matters each year.[13] With the FRCP's new requirements that attorneys meet by the 99th day of litigation to discuss discovery and produce a "location and description" document describing relevant information, attorneys must have a clear grasp on their organization's data and understand the security considerations associated with the data. General counsels will realize that discovery plans cannot be prepared from scratch for every new matter. A well-maintained inventory of data and systems is critical to their ability to comply with the amended FRCP and prevent opposing counsel from taking advantage of any uncertainty regarding their data and systems. Many security programs have a system inventory of some sort, but it is usually not business-process driven and does not contain critical discovery information (e.g. format and location of the data) or details such as whether or not the data is privileged or protected.

Product liability litigators Jennifer Smith Finnegan and Aviva Wein succinctly summed up this reality:

---

[11] "Clarity stops at the borders," *Financial Times,* Nov. 10, 2006 at 10.
[12] Fred. H. Cate and Margaret P. Eisenhauer, "Between a Rock and A Hard Place: The Conflict Between European Data Protection Laws and U.S. Civil Litigation Document Production Requirements," *Privacy & Security Law Report,* Bureau of National Affairs, Vol. 6, No. 6, Feb 5. 2007, http://www.privacystudio.com/Links%20posted%20to%20web/BNA%20-%20EU%20Data%20Protection%20Article%20-%202-2007.pdf.
[13] "Amendments to Federal Rules on E-Discovery Offer Good News for Corporations," LexisNexis Press Release, Dec. 11, 2006, http://www.lexisnexis.com/about/releases/FRCP-6-advantages.asp.

> [I]t would be prudent…for a company and its in-house legal department to take inventory of all of its electronic information systems, the kind of information created and stored, where and how it is stored, how long it is stored and how it is destroyed or overwritten during the normal course of business. The systems should also be assessed in conjunction with the company's document retention policies to ensure that the management and operation of the electronic information systems are consistent with – and do not violate – those policies. Likewise, the company's document retention policies, including its "litigation hold" provisions, should be inventoried, monitored and kept up-to-date. Finally, when litigation does arise, it would be helpful to designate an IT officer or employee, or other consultant, to serve as liaison to in-house and outside counsel to help address electronic discovery questions. The good news is, once this initial work is done and routinely kept up-to-date, the company will not have to repeat the entire exercise each time it is faced with new federal litigation.[14]

Knowing what relevant data an organization has is the first step, and preserving that relevant data is the second challenge. Under the FRCP, parties can face draconian spoliation sanctions for the destruction of data that is subject to preservation. According to one study, courts granted sanctions 65% of the times, mainly for destruction of evidence.[15] One of the "poster cases" regarding sanctions for failure to produce discoverable data is *Coleman v. Morgan Stanley,* 2005 Extra LEXIS 94 (Fla. Cir. Ct. Mar. 23, 2005), in which the judge entered a default judgment against Morgan Stanley for its failure to produce nearly 2,000 backup tapes containing discoverable emails. The plaintiff was awarded $604 million in compensatory damages and $850 million in punitive damages.

"A well-maintained inventory of data and systems is critical to their ability to comply with the amended FRCP and prevent opposing counsel from taking advantage of any uncertainty regarding their data and systems. "

Management policies set the tone for compliance with the FRCP and the management of litigation risks. Operational policies and procedures define how risk management actions will be carried out. It is imperative that companies be able to (a) quickly identify and preserve existing relevant data and (b) identify and notify persons with access to data in order to avoid the destruction of relevant data in their possession and to preserve any new data that is created from the moment that litigation commences or becomes reasonably imminent. In addition, this data must be exempted from

[14] Jennifer Smith Finnegan and Aviva Wein, *Product Liability Law & Strategy,* Nov. 16, 2006, http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1163671528626.
[15] Shira A. Scheindlin and Kanchana Wangkeo, "Electronic Discovery Sanctions in the Twenty-First Century, 11 Mich. Telecomm. Tech. Law Review 71 (2004), http://www.mttlr.org/voleleven/scheindlin.pdf.

routine data destruction processes. Privileged and protected data must also be identified and sequestered so it is not produced or revealed, thereby defeating the privilege or protection and rendering it discoverable (except , of course, this does not apply to data that was inadvertently produced and may be "clawed back" per Rule 26(b)(5)). The categorization of data in an enterprise security program as of high, moderate or low criticality (or top secret, secret, confidential) is very useful in helping counsel identify privileged or protected information. Additionally, counsel must be able to prove the integrity and authenticity of ESI and explain to opposing counsel and the court what security measures are in place to protect the data. Management policies and organizational procedures are often the best proof of these actions and processes and, therefore, play a critical role in managing the risks associated with discovery in the digital age.

In addition to the production and preservation of data, counsel needs to work closely with security personnel behind the scenes to (a) find out whether relevant data was subject to any security incidents, and (b) determine which ESI is not reasonably accessible or extremely expensive or burdensome to produce. In addition, the attorney needs to clearly understand:

- Retention and destruction policies applicable to relevant data;
- What happens when data is deleted and how it is overwritten;
- Whether metadata exists for relevant data and, if so, what it contains; and
- How often the ESI is backed up, where backups are stored, and how long they are kept.

The policies and procedures of the enterprise security program are central to each of these issues.

► THE TECHNICAL PERSPECTIVE

Numerous technical considerations come into play with the discovery of ESI, how it is handled by the receiving party, and how it is defended to the court. For example, one party may (a) accuse the other of not locating or producing all relevant data, (b) question whether the digital data produced is the same as that which was originally relied upon, or (c) contend that the system configuration has been changed since the underlying action occurred. There may be concerns that data has been deleted or intentionally destroyed and, of course, there is the possibility that in-house counsel might have no idea where relevant data is located, much less what format it is in and whether or not it has been preserved. Such a situation is especially likely if data is spread across multiple business units operating around the globe.

E-discovery can only be successfully managed if the CISO/CSO and GC work together and integrate e-discovery requirements into the enterprise's security program.

It is the organization's security program that will help address such issues. From the judge's perspective, a strong security program can be the determining factor in deciding whether to grant or deny discovery motions seeking additional data, the right to test or sample data, or the right to access the opposing side's IT systems. Organizations with good security governance and effective enterprise security programs in place are more able to prove to the court that they can identify and protect relevant data, and that they have systems and processes in place to assure the integrity of the data produced.

Effective enterprise security programs:

"E-discovery can only be successfully managed if the CISO/CSO and GC work together and integrate e-discovery requirements into the enterprise's security program. "

- Have complete inventories of digital assets (data, applications, and systems);
- Take into account compliance requirements;
- Are based on risk assessments and the categorization of assets;
- Have effective controls in place which are linked to performance metrics;
- Incorporate security best practices and standards;
- Have designated security configuration settings based on controls and categorization levels;
- Incorporate incident response, crisis communications, and business continuity and disaster recovery plans;
- Have thorough policies and procedures (including change management);
- Are implemented through effective training programs, monitoring, and enforcement;
- Are based on risk management and return on investment business cases;
- Undergo rigorous reviews and audits; and
- Ensure that identified deficiencies and weaknesses are corrected.

Certain technologies deployed in a security program can be especially helpful with respect to e-discovery. Encryption software, hash algorithms, and digital time stamps, for example, help support the integrity and authenticity of data. Software tools that detect steganography programs and malicious code can help prove the system is secure and tools are deployed to detect unauthorized acts.

The GC will require assistance from the technical team regarding the production of data in such new forms as instant messages and text messages, images and data from cell phones, information from thumb drives, and data from employees' web-based email accounts. Discovery of this nature requires an understanding of the system architecture, software tools, and capabilities available. The CISO/CSO may also offer valuable assistance in helping the GC determine the format in which electronic data should be produced. The format may be dependent upon what technical tools are available to help analyze ESI. An example of such a new tool is an audio search technology on the market, Nexidia, which creates phonetic indexes, supports 22 languages, enables searches by keyword, phrase, Boolean searches or proximity matches, and accommodates accents, dialects, and regional variations in pronunciation. While analysts have been cautious in endorsing the technology, it is clear that these types of tools can help sift through mountains of ESI, and it is highly likely that other new products will appear on the market.[16] GCs will need technical experts to advise them on the availability and usage of these tools.

Technical assistance is also needed when forensic skills and technical tools are needed to retrieve "deleted" data, determine if data has been sabotaged or manipulated, and uncover obstructionist acts. Software programs that "wipe" or erase entire hard drives are often used by individuals wanting to remove digital evidence from computers. Technical tools help uncover such acts and expose attempts to intentionally hide or delete discoverable data. For example, in one case, an executive of a software firm wiped clean an entire personal computer and then installed a Linux operating system. Forensic tools were able to uncover that the Linux system was installed after the subpoenas in the case had been issued.[17]

Of course, many companies utilize real-time investigatory tools, steganography detection software, and other forensic tools to guard against economic espionage, unauthorized acts, and sabotage. General counsels need to understand (a) the security program in their organizations, (b) the technical tools deployed by their organization and what purpose they serve, (c) the forensic capabilities in-house and available from experts, and (d) what new tools are on the market for e-discovery and how they could be used within the organization's system architecture and security program.

In summary, technical and legal considerations have never been so interwoven. One of the most prudent actions any general counsel can take after December 1, 2006, is to sit down with their organization's CISO/CSO and develop a plan to address e-discovery and the multitude of issues that can accompany ESI. This may well result in additional financial support for security programs, and CISO/CSOs may well enjoy a higher measure of respect within executive offices and the board room. General counsels may also realize that through enterprise security

[16] C.C. Holland, "Full Speed Ahead," *Law.com,* Nov. 21, 2006, http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1164029731480.
[17] David Sumner and Damon Reissman, *E-Commerce Law & Strategy,* Dec. 4, 2006, http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1164981804524.

programs and closer legal-security cooperation, (a) they have a decided advantage over adversaries in litigation, and (b) can take advantage of the amended FRCP to cut costs associated with discovery.

► CONCLUSION

The amendments to the FRCP are creating a convergence of legal, managerial/operational, policy, and technical considerations with respect to how litigation is managed, costs are contained, and integrity and authenticity of evidence is supported. Boxes of paper and Bates numbering machines for sequencing paper discovery are rapidly becoming obsolete. Likewise, the traditional attorney's mindset regarding document organization, the discovery of evidence, the sequence of interactions between counsel, the strategy of litigation will no longer be applicable. The new FRCP has thrown attorneys into the digital world, requiring them to understand security programs and technical capabilities. New security issues can now determine whether a case is won or lost. The cost of e-discovery can be managed or it can push a case to settlement. All of these factors are largely dependent upon:

- How well counsel understands the organization's security program;
- The extent to which management supports the operational shifts necessary to accommodate the new Rules; and
- To what degree best practices and standards, such as ISO 15801, are integrated into the security program.