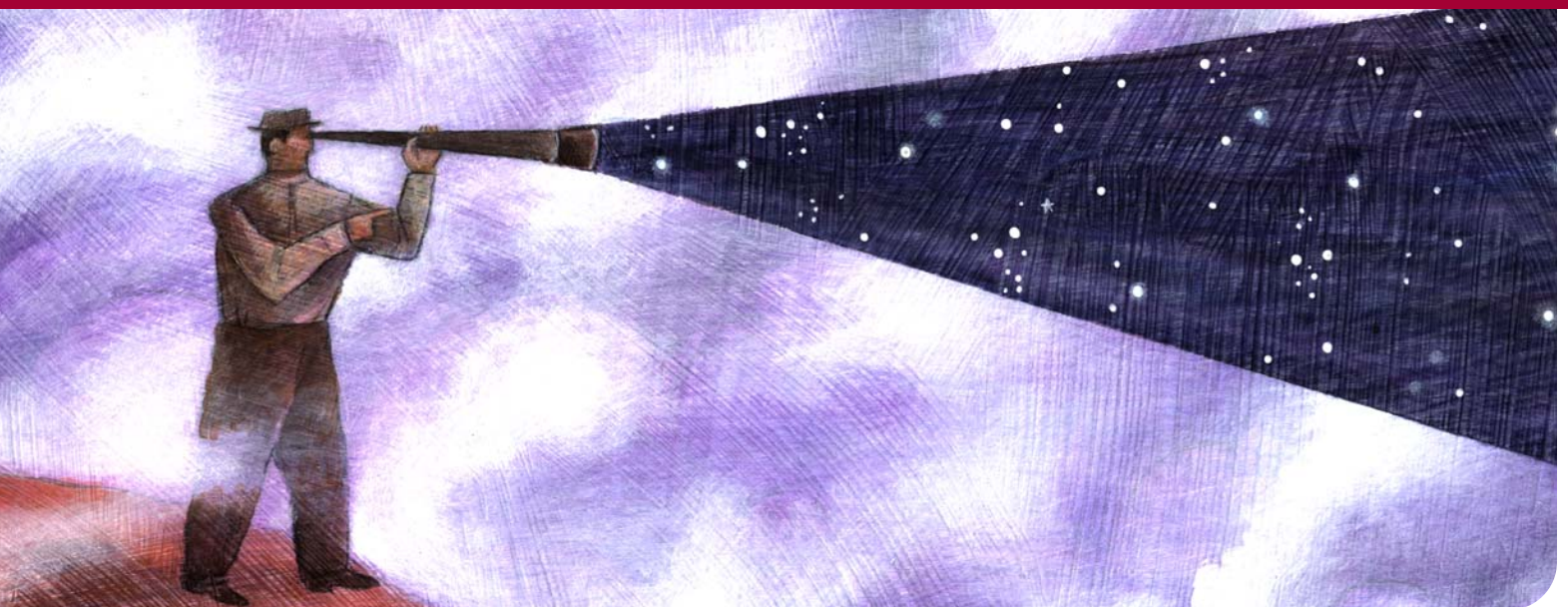


Cracking the Code on Security

December 2006



A Publication of ILTA

Inside This Issue

3 Better Safe Than Sorry: Assessing Internal Security on Your Firm's Network

by Carlos Batista of Alston & Bird LLP

A network security program is an asset to any law firm, but only if it's based on an accurate assessment of how well the network is protected. Evaluate and define your needs and give management an accurate report on your security profile.

6 Raiders of Network Security: Could a Layered Defense Have Stopped Indiana Jones?

by Klaus Majewski of Stonesoft Corp.

It's not enough just to have a strong hard-shell perimeter defense around the company if the inside of the company is unprotected and soft. Layered defenses, managed in a unified manner, can stop the most adventurous hacker.

8 Unifying Information Security Management

by John Hall of Integration Appliance

As security issues continue to grow in importance, firms that achieve pervasive information security are successfully limiting several classes of exposure and risk without needlessly disrupting or reducing the productivity of their users.

12 Planning an IS Security Department

by Atlas Lee of eSentio Technologies

The growing need to protect confidential information from destruction or e-theft motivates many firms to consider establishing an information systems security department. Basic questions need some answers before you begin.

13 Make the Right Call on VoIP Security

by Michael Oh of Heavy Water Ltd.

VoIP is being widely adopted in law firms, and it has become a serious target for hackers. Firms implementing VoIP, or planning to do so, should understand the security ramifications and prepare accordingly.

15 Is Your Metadata Showing?

by Donna Payne of Payne Consulting Group

Legal professionals must understand and eliminate metadata to mitigate risks inherent in all files formats. Recent cases, rulings and opinions that are related to metadata are "exposed" for our readers.

19 Managing the Menace of Metadata

by Randy Farrar of Esquire Innovations, Inc.

Data about the data can be as important as the data itself — possibly even more so in some cases. So seriously consider availing yourself of tools and strategies to harness metadata.

20 The New E-Discovery Rules: Take the Lead in Ensuring Compliance

by Faith M. Heikkila of Pivot Group

As part of an IT team, you can look forward to fielding questions and requests from your litigation practice group as to electronically stored information (ESI) formats that exist within your firm and within your clients' systems as we face the new rules for electronic discovery adopted as part of the Federal Rules of Civil Procedure (FRCP) went into effect December 1, 2006.

Statement of Purpose: ILTA is the premier peer networking organization, providing information to members to maximize the value of technology in the support of the legal profession.



EDITOR'S NOTE

Security vulnerabilities and breaches are proliferating, and we see misdeeds make the headlines daily. Law firms have a particular interest in securing systems and data, as their information stores include internal data, intellectual property and the confidential information relative to their clients' needs.

Our authors share their expertise on a broad range of security topics, from tighter physical security of networks and specialized systems, metadata "scrubbing," understanding the new federal rules regarding preservation of electronic records and everything in between.

Enjoy the read as we escalate your knowledge of security issues.

Ken Hansen, Editor

ABOUT ILTA

Providing technology solutions to law firms and legal departments gets more complex every day. Connecting with your peers to exchange ideas with those who have "been there done that" has never been more valuable.

For nearly three decades, the International Legal Technology Association has led the way in sharing knowledge and experience for those faced with challenges in their firms and legal departments. ILTA members come from firms of all sizes and all areas of practice, all sharing a common need to have access to the latest information about products and support services that impact the legal profession.

by Carlos Batista of Alston & Bird LLP



:: Better Safe Than Sorry: Assessing Internal Security on Your Firm's Network

An integral part of any law firm's information security program is the ability to assess the state of its own security. A fresh, invaluable and objective appraisal can be performed by an authorized vendor; however, consulting fees can be costly and therefore difficult to sell to management. Doing the assessment yourself can be both cost-effective and a real value to you and your firm, but you must plan appropriately.

This article offers a practical approach for conducting your own security assessment, including how to plan and perform it, how to collect and analyze the results and how to avoid some of the pitfalls along the way.

Planning Your Security Assessment

Careful planning is the first and most important step of any security assessment. While it may be tempting to break out your network security tool kit right away and begin scanning the entire network, this can lead to haphazard information collection and analysis and provide practically no basis for attaining consistent measurable results. Following are the three key steps to proper planning:

Establish a reliable grading system. How will the assessment results be graded? Will you use a scale from 1 to 10, a "low, medium, high" vulnerability chart, an academic grade scale or a color-coded scheme? How many types of vulnerabilities can your resources have and still receive a certain grade level? Which vulnerabilities are more critical than others?

Grading: Quantifying the results of your assessment is critical, as it gives your assessment process continuity over time and provides key metrics to evaluate how your security improves (or worsens) when new variables (such as a system addition or upgrade) are introduced. For example, you may find that the assessment uncovered five vulnerabilities in your Web server during one assessment, giving it a grade of "6." Sometime before the next assessment you install an

intrusion prevention system (IPS). When you perform a second assessment on that Web server, it uncovers only one vulnerability, qualifying it for a grade of "8." You can now demonstrably show that your security has improved over time, as well as provide firm management a measurable ROI for your IPS.

Scope: Determining the scope of the assessment is also critical: What resources or information assets are going to be the focus of your assessment? You can choose to make the scope small, such as a specific client portal or one of your Web servers, or you can make it large and choose to assess your entire network.

Security isn't achieved through technical means alone. Evaluate any administrative or procedural controls that are in place, as well as what physical controls, if any, exist (*i.e.*, cameras, security guards, building access systems).

Following are some key information resources or processes you may want to target or assess specifically:

- Perimeter network, including firewalls, DMZs and IDS/IPS
- E-mail system, including SMTP gateways, connectors and e-mail service providers (ESPs)
- Document management system
- Litigation support databases
- Client portals, extranets or electronic "deal rooms"
- Network operating system security
- Desktop operating system security
- User provisioning/deprovisioning process and procedure
- Administrator access (who has it and do they need it?)
- Help center and technical support processes
- Password management

Patch management

Physical access to information resources (data center and/or office space)

Avoiding Common Pitfalls

Short of failing to have an overall assessment strategy and scope, one of the biggest mistakes you could make is not communicating the assessment action plan to your constituency. Make sure you give your IT department or leadership plenty of notice before you begin performing vulnerability scanning or penetration testing on your network. The last thing you want to have to explain to your firm is how half of the servers went down during an unscheduled penetration test.

Use your change management process as much as possible to coordinate any vulnerability scanning. There are, however, possible exceptions to this rule. For example, you may not want to notify your helpdesk staff in advance that you will be calling the main helpdesk number randomly from various offices to see if they will give you a user's password over the phone.

Also, avoid a common mistake made by security assessors that involves managed service providers. If you use a managed service provider to host services such as your website, spam filtering, managed intrusion detection/prevention and payroll automation, think twice before running a penetration test against them. Why? Because unless your service contract explicitly authorizes it, you are generally prohibited from performing any security scanning or penetration testing on a managed service provider. This might lead to prosecution by your managed service provider for attempting to hack into their network — or worse, actually causing a service outage. Sidestep that possibility by requiring your service contracts to contain language to provide your firm adequate relief should the service provider ever be compromised in a way that negatively impacts your firm.

Tools of the Trade

Once a methodology has been selected and stakeholders notified, the assessment can begin. Following are tools you can use to perform vulnerability scanning on certain kinds of resources. Make sure you have authorization to proceed before running these. If configured in a certain way, some of them may actually find and exploit vulnerabilities automatically, potentially causing a service outage.

Public Databases and Repositories: You can obtain a wealth of information about your firm just by consulting the various major online databases such as Domain Name System (DNS) entries and domain registration records. Examples include www.dnsstuff.com, www.sampspade.org and Whois databases such as whois.org and whois.arin.net. The ARIN and registrar databases can be especially valuable to a hacker if actual contact names are listed beside the registration records. He potentially could use these contact names in a social engineering attempt directed toward your firm or your network service providers.

The website www.internalmemos.com is loaded with confidential internal memos posted by employees working in companies all over the world. While it's a paid service, some of the older memos can be viewed free of charge. If you look closely, you can find several large law firms mentioned there.

Additionally, Google's search engine can be used as an effective hacking tool to find vulnerabilities which can be used to access information without authorization. (See <http://johnny.ihackstuff.com> for more info.)

Port Scanning: Few will argue that Nmap (www.insecure.org) is the fastest and most efficient port scanner and footprinting tool available today — and it's open source and free. This open source utility can be used to scan for operating system versions, open ports and services on your perimeter and DMZ networks and will give you a solid basis for determining attack vectors, if any exist, and what tools to use next.

Vulnerability Scanning Tools: There are many tools available for scanning and reporting vulnerabilities on nearly any type of host, whether they are servers, desktops, routers or switches, firewalls, applications such as e-mail, Web and SQL. The trick is to use the right tool for the right system. Some of the more popular and effective tools include:

Nessus. The “Cadillac” of all vulnerability scanners, it can scan for vulnerabilities on your firewalls, DMZ networks, Windows/Linux/Unix hosts, as well as major Web servers like Apache and IIS and others. For reporting, ease of use or event correlation, look at offerings from McAfee's Foundstone product line or Qualys. The downside is that they require greater capital investment.

Microsoft Baseline Security Analyzer (MBSA). Microsoft's tool for analyzing the patch status of your environment is a must for any organization using Microsoft products and should be a part of your ongoing security operations whether you're performing an internal assessment or not.

WebInspect. An excellent tool for analyzing Web-based applications, it does a solid job of not just looking for vulnerabilities in unpatched binaries, but also in detecting coding errors that would allow for more sophisticated attacks such as cross-site scripting or SQL injection.

RootKitRevealer. An excellent tool from SysInternals (just purchased by Microsoft) used to detect rootkits installed on Microsoft hosts.

NetStumbler. Detects information on security, signal strength and names on wireless access points (WAP) currently available. Great for detecting unauthorized WAPs.

Cain & Abel. It's LC5's (L0phtcrack) heir apparent in the password cracking category. It can actually sniff the network for password hashes and attempt to decode them using brute force dictionary attacks.

WinPcap and Ethereal. These are two very effective and very free network sniffers you can install to capture and analyze network packets.

Telnet. It's been around for a while but still can be a great vulnerability testing tool, particularly for routers and switches. It can also be used to look for vulnerabilities and open relays on SMTP servers.

Cisco Router Auditing Tool (CIS RAT). CIS RAT can be used to load a config file from a Cisco router and compare it to a security template to ensure that the router is configured to a set security standard.

Other Tools and Techniques. Many other assessment tools exist, including war dialers to scan for dial-up points of presence and wireless network sniffers like AirSnort, which can be used to crack WEP keys.

If you're assessing operational security features, perhaps your most effective tool will be a face-to-face interview. Schedule some time with the owners and users of a specific data process (e.g., creating user IDs or installing servers). Ask pointed questions regarding the security of those processes. For example, you may want to ask the person(s) responsible for building servers if they use a standard build document or process. Do they disable key applications and services out of the box; place a security banner on the server, etc.? Be sure to review any documentation associated with the build or process.

Finally, don't overlook the telephone. It's often a hacker's best tool for getting access to confidential information simply by calling and asking for it. Use it yourself to test the overall operational security of your helpdesk and IT staff, as well as your users, to ensure they're not giving or receiving passwords over the phone.

Prepare and Present the Results

Depending on the scope of your security assessment, the raw data you collect can amount to hundreds of pages of data about open ports, scanned IP addresses and discovered vulnerabilities. Based on your planning prior to actual assessment, you should be able to sort through your firm's vulnerabilities and determine which are the most critical and should be remediated first. Critical issues should be at or near the top of your report, followed by ones deemed less critical. Following are some useful tips for preparing and presenting your findings:

Keep your report brief. A 20 to 30-page report should be sufficient for most law firms. Leave the raw scanning data out and save it in a secured network location or offline on a CD or DVD for review by the technical team later.

Prepare an executive summary. A two-page executive summary should provide an adequate analysis of your findings.

Organize and consolidate your findings wherever possible. If you've discovered 50 percent of your servers are missing patches, remark that your patch management process is an area of concern rather than list each server.

Note areas of success as well as for improvement. The report shouldn't be all "bad." Discuss strengths you found, too.

Rank yourself fairly and objectively. When assigning scores or rankings to your results, be as objective as possible. Unmerited high rankings may result in fewer resources being allocated to correct actual problems in the future. Consistently low rankings may lead to questions about why your security program is so unsuccessful. It pays to be candid.

Suggest a timeline for addressing discovered vulnerabilities. Or at least define a level of difficulty for addressing them. For example, "installing the MS04-011 patch on two servers" may be rated as "easy," whereas "defining new password policies and security standards" might be rated as "difficult."

Think about your firm as a business. How can your discovered vulnerabilities affect your firm as a whole? How do these vulnerabilities increase the firm's (or a specific practice group's) level of risk in certain areas, and what should be done to address those risks?

Don't be afraid to say what you think. If you believe your firm could benefit from an identity and access management framework, two-factor authentication or information rights management, say so! A security assessment is the ideal opportunity to present new avenues of direction to your leadership in a forum where they are expecting to hear just that.

Present your findings in person. When you deliver the report, make an appointment with management to discuss the findings and answer any questions. These meetings can be invaluable in gaining immediate feedback on your findings and encourage brainstorming on future ideas.

Involve your loss prevention partner(s), if possible. An LPP can be a very vocal advocate for security initiatives to assist you in effectively articulating the reasons why not addressing security problems could increase the risk of data loss to your firm.

Address Your Findings

Once you have presented your findings and received feedback from firm leadership, go back and actually address the vulnerabilities you discovered. Create a project plan for getting the most critical vulnerabilities closed or otherwise mitigated, and set a date for your next internal assessment. Doing so will encourage you and your team to address what was found before performing the next assessment. If you do manage to resolve a good deal of the outstanding issues based on your planning and assessment strategy, you should be able to see marked improvement on your next assessment.

Evaluate Your Assessment Program

Conducting your own internal security assessment won't be quick or easy. But spending an appropriate amount of time and resources at the outset to understand what you're trying to assess and then developing a methodology on how to assess it will make your findings more meaningful in the long run. Moreover, keeping your grading standards consistent will give your assessments greater value and reliability.

Security will always remain a moving target, so standards may have to be adjusted along the way. Finding and using the right tools to perform the assessment will also give you a big advantage in discovering vulnerabilities. However, don't rely on technology alone to help you uncover vulnerabilities. Speak with others in the firm regarding how data is handled, and do not discount the value uncovering and mitigating social engineering.

When it comes time to present your findings to your leadership, do so in a way that makes sense to them. Avoid techno-speak as much as possible, and suggest ways to address your findings with solutions that make business sense. This is your opportunity to speak up about information security risks both today and in the future. Don't be afraid to propose markedly different courses of action regarding information security.

And finally, follow up on your findings. Take steps to address as many of those vulnerabilities as realistically and methodically as possible. The assessment process may seem tedious, but you can be confident that the time and effort you put into enhancing the security of your firm's network will pay off in many ways. The firm's management, loss prevention partners, and you, will sleep better at night.



by Klaus Majewski of Stonesoft Corp.

:: Raiders of Network Security: Could a Layered Defense Have Stopped Indiana Jones?

Consider intrepid adventurer Indiana Jones and his continuing quest to acquire archeological artifacts as a metaphor for potential threats to your network. Throughout the film trilogy, Jones must make his way through a series of obstacles and booby traps before he can reach some kind of valuable treasure. Each system of traps employs various methods for stopping intruders. It's a system of layered defenses.

The designers of these devices could have constructed a system to protect their treasures that used the same kind of trap over and over again. This would have increased the depth of defense, but once Jones found his way around a particular trap, it would have been easy for him to defeat it each time. So, they cleverly added more variety in both depth and breadth to the layers of protection mechanisms. Judging from the number of skeletons that Indiana Jones passed along the way to his destination, it seemed to be an effective combination; although in Jones' case, the traps merely served to slow him down a bit.

The defensive layers in these movies were static, and no one was coordinating their activities. Imagine how much more challenging it would be for Jones to steal the treasure if each defensive layer would trigger an alarm and someone coordinated the rest of the traps. For example, the defenders could have put more snakes in the area as soon as they recognized Jones and knew of his terrible fear of snakes.

Advantages of a Layered Defense

The same principles hold true for layered defense systems in modern network security. It's not enough just to have a strong hard-shell perimeter defense around the company if the inside of the company is unprotected and soft. Once an intruder penetrates the perimeter defenses, there's nothing else to protect company assets. The e-proowler can roam freely, hunting for the buried data treasure.

It would be useful to be alerted to the intrusion and have some way to slow down the intruder — even catch him. If he can't be caught, then at least we should get enough evidence of what he did and how he did it. Thus, we can modify and improve our defenses to prevent future intrusions.

With respect to network security, a layered defense can help us reach all of these goals. Adding layers (depth) to a defense strategy is easy if you can use the same product over and over. For example, you can add additional firewalls inside the perimeter to protect sensitive networks like research and development or accounting.

A combination of depth and breadth of defense is needed for better protection. You can add several protection methods onto each layer. Examples include:

Perimeter layer - Firewalls, content checks for attachments

Network layer - Intrusion detection systems, Web proxies

Host layer - Antivirus programs, personal firewalls

Managing a Layered Defense Can Be Challenging

Many companies already face resource challenges with respect to security administration. Security products typically have their own management interface. This means that administrators have to learn several different products and user interfaces. It's almost impossible to enforce consistent and coherent security policy across all products. The risk of human error increases when administrators have to switch between the user interfaces and different configuration methods.

In addition, these products are not necessarily designed to work together. If there's a problem, the administrator has to collect incompatible information from several different resources and try to

form a big picture of the incident manually. This takes a lot of time and resources.

Managing multiple products from multiple vendors in each layer without adding any operational cost means the already busy security administrators will have even heavier workloads. Unfortunately, they may not be able to cope with the excessive workload, and eventually some tasks may be dropped or missed. This endangers the entire security environment.

Unified Management to the Rescue

But don't fear, the complexity of managing a layered defense can be solved. Every security device in each layer of defense should be managed with an integrated and unified management system. The first aspect in unifying management systems is that the configuration of each device should be based on the same basic concept. This ensures that the data used in configuring security devices is consistent and coherent, which in turn reduces the likelihood of misconfiguration and human error. For example, using unified management, an administrator can define objects just once and use them in several different places rather than redefining them every time.

Events generated by security devices (*e.g.*, logs, alerts) should have a common structure so that the information can be centrally collected and processed. Reports based on the consolidated information will give more refined information to administrators and speed up their problem solving, leaving more time for other business-related tasks.

A unified management system optimizes resources. Several studies show that the three-year total cost of ownership (TCO) of a security solution consists mainly of administration costs. Most of the administrator's time is spent on making changes to the existing environment and investigating possible security incidents. A unified management system allows administrators to centrally upgrade security patches to all security devices in different defense layers. Change management becomes easier and more accurate because configuration changes have to be done only once and then they can be applied to several different enforcement places.

Layered Defense: Deeper, More Effective Security

Unified management reduces the number of the false alarms because the alarm information can be correlated to information received from other enforcement points. For example, firewall logs show some suspicious activity against host A. The administrator can use unified management to check intrusion detection system logs and host A syslog entries from the same time period and see if the alert was real or not. The fact that all this information is in one place saves time and money. The administrator can then concentrate on incidents that are real and need attention.

Layered defense is a battle-proven way to increase the security of your network. At one time it was a privilege that only big companies could afford, but now with unified management and optimization of resources, small and medium-sized businesses can afford it, too. And with unified management of the defensive traps, even Indiana Jones can be stopped.



Layered defense is a battle-proven way to increase the security of your network.





by John Hall of Integration Appliance (IntApp)

:: Unifying Information Security Management

Security is one of the broadest and most challenging issues facing legal IT organizations. Unlike the traditional IT activities focused on enabling business efficiency, security adds the specter of active attack and ever-present risk.

Just listing all the potential threats against which IT must protect their organizations is enough to make any CIO nervous. Security covers a wide range of hazards including network intrusion, malicious software such as spyware, viruses and e-mail phishing. Furthermore, the proliferation of newer technologies such as wireless communication and the emergence of next-generation attacks like vishing (<http://tinyurl.com/fttb3>) further complicate the security landscape. To protect their firms, IT organizations commonly rely on firewalls and other network defenses, operating system and e-mail scanning software, patch management solutions to keep systems up to date, secure communication technologies like encryption and VPNs, and of course, user education.

These examples comprise just one class of security problem: attacks originating outside the firm. Organizations must also defend sensitive information from inappropriate *internal* access.

In this context, the overarching challenge is to provide users with the information they need to be productive while keeping sensitive information out of the wrong hands. As security issues continue to grow in importance, firms that achieve pervasive information security are successfully limiting several classes of exposure and risk without needlessly disrupting or reducing the productivity of their users.

The Importance of Information Access in Law Firms

At their very core, law firms are in the expertise business, producing and delivering intellectual property and information to their clients. As

part of the creative process, it's important that internal stakeholders have access to information. Such access may take the form of a shared document repository used to streamline the collaboration process. Or it may mean using more sophisticated tools to identify and leverage reusable assets for greater attorney efficiency and productivity.

Indeed, the latter class of sharing has earned its own category label: Knowledge Management. KM approaches and best practices occupy a great deal of thinking, experimentation and effort on the part of many law firms. At its most fundamental level, the KM thought process focuses on how to share information within a firm. This information includes work product as well as metadata such as staff skills, expertise and experience.

In a June 2006 ILTA white paper on KM, David Hambourger succinctly defined a key goal of KM as "capturing, organizing and storing knowledge and experiences of individual workers and groups within an organization and making this information available to others in the organization." (<http://tinyurl.com/hmult>)

By breaking down the barriers to information, firms hope to increase internal efficiency through skills sharing and the reuse of IP, to improve client service and satisfaction through increased productivity and to maximize new business opportunities. To support this, several vendors offer legal-specific tools and repositories that can help firms add structure to the way they store and manage key information and help users quickly find relevant information throughout the organization. For example, applications such as enterprise search make information that's readily available accessible to those who might benefit from it, much in the same way that Google allows people to connect with publicly available Web pages relevant to their needs.

The Information Security Paradox

The goals of knowledge management highlight a paradox with regard to information security. On one hand, given significant potential benefits, firms are spending energy and resources to open up access within the organization. On the other, there is a good deal of sensitive information within the firm that should *not* be generally available. In some instances, this information is routinely locked down as a matter of policy and practice. For example, staff e-mail accounts are protected from general access through the mandatory use of passwords.

In other instances, however, a “security through obscurity” approach may be the only defense used against unwanted internal access. These cases include instances where sensitive information is stored in repositories that are generally accessible, amidst large volumes of information not considered sensitive, such as a firm’s document management system, wherein sensitive information may be accessed either with inappropriate intent or accidentally. In other cases, firms may forego using applications designed to streamline the creation and management processes, because even when security controls are initially put in place, stakeholders feel that the risk of inadvertent disclosure or access is too great.

Certainly, the legal technology landscape is ripe for a more unified approach to managing information security, owing to the proliferation of information repositories; the decentralized management of these storehouses and their access controls; and the increasing use and sophistication of search, portal and other KM technologies designed to connect people with information throughout the firm. In such environments, firms that do not successfully control access to private information face significant risk.

Key Reasons for Information Security

Several factors drive the need for access controls, including firm conflicts, litigation issues and confidential matters. Each creates the need to secure information, but the drivers and the implications of failure for each differ.

Conflicts and Ethical Walls

Firms often create security barriers in the form of ethical walls to manage conflict of interest situations. A prime example of a conflict is a firm seeking to represent adverse parties. Firms perform conflicts checks to identify these situations when taking on new business in order to address and resolve them immediately.

Consider a hypothetical example where a firm representing The Coca Cola Company merges with a firm representing an independent bottler. In situations where clear conflicts exist, absent client consent the merged firm would have to part ways with one client because the combined organization could not serve two competing masters. These types of conflicts may also arise when a firm takes on a lateral hire from another firm who represented a party adverse to an existing client.

When such situations arise, firms often approach both clients and ask them to sign a waiver consenting to allow the firm to continue representing both companies. In these cases, firms often emphasize their use of ethical walls as a way to assuage client concerns, arguing that placement of such intrinsic barriers will prevent attorneys from

accessing or being exposed to materials related to the adverse party’s interests and activities.

In practice, there are situations where a weaker or potential conflict may be judged to be manageable absent client consent, and the firm may decide that a waiver is not required to take on the business. Instead, firms may still set up an ethical wall as a protective measure. In these cases, there remains the risk that the relationship or potential conflict may be discovered in the future and the firm will need to explain its behavior before a judicial audience. Therefore, the organization must always be prepared to demonstrate that it used sound judgment in acting absent explicit waivers and that it put sufficient protections in place to control access to sensitive information.

Ethical walls have become a hot area of focus for several firms — not surprising, given current growth trends in the legal industry as merger activity continues, lateral hiring practices grow more aggressive and firms work to expand the scope and range of services they offer their clients. In some instances, insurance companies have even set requirements for firm ethical wall security practices.

All of these situations highlight the need for rigorous information security management. Courts are also catching up and increasingly accept ethical walls as a suitable way to manage conflicts. (<http://tinyurl.com/hd9rl>)

Litigation Issues

In the context of litigation, two key scenarios highlight the need for a coordinated approach to information security and management.

Litigation holds: Law firms have existing policies and procedures with regard to the treatment of records. These typically include enumerated destruction policies. When the firm becomes the subject of a lawsuit, it has a duty to prevent the destruction of relevant information which may be responsive to discovery requests by placing a litigation hold on such material. In these cases, information security shifts from preventing access to preventing deletion. These scenarios also call out the need for logging of such restrictions so the firm can demonstrate compliance.

Protective orders: Often employed in the context of trade secret litigation, protective orders typically are used by adverse parties to enable firms to communicate confidential client information which may not be disclosed publicly or may only be viewed by attorneys and not their respective clients.

Such orders prescribe the ways in which different kinds of information must be designated and labeled. They also outline handling practices such as the treatment of physical records and staff access protections. For instance, such material may only be accessible to staff officially assigned to work on that particular case and only after they have read and signed the protective order.

When information subject to a protective order is incorporated in legal work product created by the firm, the firm must take steps to ensure that general access to such documentation is restricted across its systems.

Confidential Matters and Security Screens

Firms must control access to internal business or client information. Firm confidential information may include:

Firm legal activity: Firms typically do not want the information created by their own internal legal representation to be readily accessible. Consider cases where the organization itself or an individual partner is the subject of or plaintiff in a lawsuit.

Business restructuring plans: Organizations keep strict control over information and documentation concerning potential business plans such as mergers or other restructuring.

Lateral hiring pursuits: Pending lateral hires from competitors are similarly sensitive activities necessitating limited internal exposure.

Compensation and shareholder performance: Business performance metrics represent some of the most confidential information within the organization, warranting the tightest controls.

Importantly, restrictions on information associated with these activities must prevent access not only to specific work product and records but also to activity logs of participating stakeholders. For example, for firms that assign matter codes for internal projects, if a time entry system is open from a security standpoint, it may report to anyone who is watching that certain timekeepers are entering time reading “legal implications of firm partnership restructuring.” Whether the documents and work product of the analysis are available or locked down in the DMS does little to put the cat back in the bag.

Similarly, clients may have special requirements for firm information handling practices, especially with regard to how information is accessed and communicated within the firm. These may include:

High profile/PR sensitivity: Organizations or individuals may have special concerns regarding potential press leaks, even those that only reveal the fact that they have solicited legal advice. Or they may have increased emotional needs for assurances of heightened security.

IP of utmost business value: Clients from industries such as pharmaceuticals, where the mistreatment of intellectual property such as patents or trade secrets may have dire consequences, also may have special information security requirements.

Regulatory controls: Various regulations and statutes such as HIPAA, *Sarbanes Oxley* and SEC rules may drive clients to insist on greater protections as well as increased logging and audit practices.

Client customer requirements: Similarly, clients may have obligations to their own customers or partners with regard to the way customer data may be handled when communicated to third parties including counsel.

Additionally, client concerns may be as simple as a basic desire that their materials not be generally accessible to hundreds of uninvolved attorneys and support staff. Indeed, it is not unusual to see clients require firms to document their information security practices as part of responses to RFPs. In some cases, clients have even commissioned external audits of firm information security practices.

In the cases of conflicts or confidential matters, information security is an area where firms can differentiate themselves from their competition, much as when a bank highlights its physical security protecting customer safe-deposit boxes. Indeed, ethical walls and security can be key factors that ease client concerns about conflicts or confidential matters and preserve their business for the firm.

Securing Against Suspicious Activity

The final area of concern in the context of information security is staff activity. Assuming adequate restrictions are in place, these scenarios arise when internal staff access public information in ways that may indicate potential problems. For example, unusually large checkout activity within a firm’s document management, CRM or other systems may indicate a pending lateral move by an attorney. Likewise, a situation where an employee who traditionally makes no copies suddenly starts making thousands billed to general overhead may warrant investigation.

The Technology Challenge

As new tools to store, manage, find and communicate information continue to proliferate, so do the challenges in managing security across them. Information security is a difficult proposition, complicated by both technical as well as environmental factors:

Proliferation of data stores: Sensitive information doesn’t just reside in document management libraries; it also lives in records, CRM, e-mail, time, accounting and other applications.

Diverging security standards: These repositories typically implement their own individual security paradigms and lack native support for external management of specific users, groups and granular access controls over stored data.

Decentralized management: The lack of application security standards and integrated management across applications forces organizations to set security manually on a per-application basis.

Decentralized ownership: Complicating matters, applications are typically owned and managed by different stakeholders, often in different departments. The conflicts/records group may define ethical walls and direct IT to configure the DMS, but no one may be worrying about locking down other applications. Such *ad hoc* approaches create scalability challenges for organizations looking to implement complex information security practices.

Rapid pace of change: Securing information means more than locking down access to a document or resource across multiple systems, it also means keeping those restrictions up to date in response to business and staff activity.

In the case of an ethical wall, for instance, IT may set security in the DMS when the firm takes on a new client, restricting attorneys working for an adverse client from accessing those materials. But the fluid nature of the practice of law means that attorney team composition changes frequently. How is that ethical wall definition kept up to date when a new attorney begins working on a matter subject to a wall? In practice, wall definitions are accurate at the start of the process, but often grow stale given the realities of the practice of law.

Approaches to Information Security

There are several approaches firms can take to manage and enforce information security, including:

Manual updates: In theory, organizations can develop better notification and enforcement processes to restrict access across repositories. But in reality, the complexities of notification requirements, distributed application ownership and maintenance challenges can create significant obstacles to the effectiveness of this approach.

Custom developed tools: Firms can develop custom security enforcement tools in house. The scope of development would be significant, necessitating the creation of security modules for key applications, linkages between modules, an interface for policy definition and appropriate notification, logging and reporting mechanisms. In practice, the resources required to design, build and maintain such tools on an ongoing basis would likely create new IT challenges for the organization.

Third-party application tools: Several third-party security enforcement tools exist. These typically focus on specific tasks or uses. For example, several vendors provide ethical walls enforcement tools. While these are functional, most do not meet the modern security needs of a law firm. For one, they only secure the DMS, not all locations where sensitive information resides. They also typically do not address maintenance challenges associated with responding to user activity. A tool-level approach may also result in security gaps and lead to additional IT implementation and maintenance challenges.

Security management platform: Nowadays, firms increasingly are adopting more stringent security practices. These include automating the creation of ethical walls for conflicts and security screens for confidential matters, enforcing security across multiple applications and monitoring staff behavior in real time to ensure accurate maintenance. The most effective way to achieve success is through a unified approach, using a single platform to monitor, update and enforce controls throughout the firm.

Unifying Information Security Management

Whether firms choose to improve security management by streamlining manual processes, building internal tools or deploying an integrated management platform, all organizations will need to address several nontechnical issues which will influence the success of the initiative:

Defining security relationships: Setting rules and procedures for defining and implementing security policies.

Setting stakeholder responsibilities: Deciding and documenting which parties own what parts of the enforcement process and their specific duties.

Educating stakeholders: Making sure that firm staff understand policies and practices; ensuring that stakeholders understand how security is enforced in their environment; providing a process for change for predictable situations (“I should be able to access this, to whom do I plead my case?”).

Alerting users: Notifying users of implementation of new security restrictions that affect them, and warning administrators when a self-maintaining security application resets a setting a user attempts to override.

Ensuring traceability: Establishing rules for logging, auditing and reporting on security walls and related user activity.

Bottom Line: Firms Can Have Broad Access and Greater Security

With the right approach, tools and education, firms can have it both ways. They can lower barriers to information access while improving protection of sensitive information. Interestingly, and perhaps counter-intuitively, controls that keep information out of the wrong hands are often enthusiastically welcomed by attorneys. In an environment where new tools make it possible for people to search out or stumble upon information they shouldn't see, attorneys often live with unsettling uncertainty. The unintentional breach of an ethical wall is not a daily experience for most firms, but for those who are involved, the repercussions are not easily forgotten.

Indeed, in most instances, timekeepers and staff will appreciate being able to search out and access internal information without fearing they will see something they shouldn't. And firm clients and management will rest easier knowing that sensitive information is secure wherever it resides.

Interestingly, and perhaps counter-intuitively, controls that keep information out of the wrong hands are often enthusiastically welcomed by attorneys.

:: Planning an IS Security Department

by Atlas Lee of eSentio Technologies

As the volume of confidential information housed in firm computers increases, so does the need to protect it from destruction or e-theft, motivating many firms to consider establishing an information systems security department. If yours is one of them, you'll have lots of questions to ask — and answer — before developing a proposal. Let's start with three of the most basic:

Why does my firm need it?

Who in my firm should staff it?

Where does the department report?

Why Do We Need It?

Physical security in a law firm is usually relegated to building property management, but IS security is solely the firm's responsibility. Information may be stolen with no trace of the theft. Such losses can be far more costly to the firm than those of even the costliest physical assets.

As important as technology is in protecting your invaluable data (and as sizable an investment as the hardware and software can be), it is only as successful and cost-effective an investment as the security organization that implements and oversees it.

How Is the Department Organized?

The core team usually consists of a manager and technical specialist. They work closely with the IT technical staff and various other individuals and departments within the firm. When putting together an information systems protection program, security policies must be authored by a designated individual well-versed in both business and IT, in order to make the policies practical and enforceable. Some of the policies will pertain to technical aspects where in-depth knowledge is required; some will involve the human resources department and other departments.

Other members of the department should be chosen to add specialized knowledge of various security measures. Among their duties will be reviewing firewall logs and intrusion detection/prevention system logs, and determining whether there has been an intrusion. They should receive security alerts issued by manufacturers or independent security organizations, and ensure that all systems are patched in a timely manner. They should also track exploits that could be used to expose the vulnerabilities due to new weaknesses revealed by manufacturers or security organizations like CERT and Security Focus.

Where Does Security Report?

That depends. Each organization's particular organizational structure may dictate, or at least influence, the decision. But customarily, the IS security department is part of IT, reporting to the CIO. Other options are for the department to report to the CFO, COO or Risk Management Partner.

So ...

When planning an IS security department, as when embarking on any new project, asking the right questions at the start will lead to the right answer at the end. The above three questions are only the first step in what should be a carefully thought-through process of forming your security department, but armed with the answers, you're off to the right start.



:: Make the Right Call on VoIP Security

by Michael Oh of Heavy Water Ltd.

Acceptance and adoption of Voice over IP (VoIP), the technology that allows telephone calls to be made via the Internet, is skyrocketing in law firms. In ILTA's 2006 Technology Survey, 23 percent of respondents reported that their primary phone systems is IP-based — a figure expected to increase dramatically in 2007.

Given this proliferation, it's not surprising that VoIP now appears on the SANS Institute Top 20 Internet Security Targets, a consensus list of top vulnerabilities for 2006 compiled by experts in the field, sobering recognition that VoIP has become a serious target for hackers.

Clearly, then, firms implementing VoIP, or planning to do so, should understand the security ramifications and prepare accordingly.

The Good News

Given its many advantages, firm-wide VoIP implementation is certainly worth considering. With the right software, such VoIP-enabled devices as softphones, wi-fi mobile phones and PDAs allow users to talk with multiple people anytime, all at the same time 24/7. VoIP fills in the communication gap by allowing firms to conduct online meetings from all their various locations with such added features such as Web cameras for visual communication. No doubt about it, Voice over IP is here to stay, and it makes sense for many firms.

The Not-So-Good News

But as functional as it can be, VoIP carries a double-whammy of security risk. First, it inherits vulnerabilities from the network infrastructure it rides upon. And second, VoIP equipment itself has built-in soft spots — a situation compounded by the fact that as the technology rapidly matures and the number of new VoIP and IPT (IP Telephony) devices proliferate, users and their firms are increasingly at risk to hack and attack through the components that comprise the VoIP infrastructure: the IP network, call servers, gateways and subscriber terminals, each with its own vulnerabilities.

Following is a brief look at each component to demonstrate the breadth of security challenges that come into play.

IP Network: The infrastructure that carries the data, voice and video in a converged environment; the backbone that includes LAN, MAN, WAN and remote access.

Call Servers: Essentially set up and monitor calls, as well as maintain dial plans, deliver basic telephony functions and authorize users — all the traditional aspects of PBX systems. They also control call signaling, phone number translations and signaling between media gateways.

Gateways: Responsible for call origination, detection, analog-to-digital conversion of voice and creation of voice packets. Media Gateways

handle translation between the IP network and the PSTN (Public Switched Telephone Network), and IP/PBX Gateways do so for SIP or H323 signaling to traditional PBX.

Subscriber Terminals: IP telephones (softphones and hardphones), available in ever-increasing forms. Softphones reside on the computers, while traditional hardphones come in multiple forms. An IP phone may even be a mobile phone connected to the network via wi-fi.

Protecting Your Back with Redundancy

Any infrastructure built to include support of VoIP must have redundancy and resiliency designed in at all levels. This is true for VoIP equipment itself, as well as for the network that supports it (including the WAN that carries VoIP to the regional offices).

IDF closets must be able to provide redundant power on the switches, redundant UPS and multiple circuits into the IDF. The switches themselves should be stackable and healable in the event of a loss. And spare ports should be designed so that the loss of a switch doesn't mean total downtime until that switch is replaced. The connectivity to the core from the IDF should have multiple links from multiple switches at both ends.

There should be multiple core switches with resilient routing dynamic protocol, multiple entry points for the call servers, media gateways and others directly related to VoIP and for others that affect traffic indirectly, such as firewalls.

And finally, data center systems such as UPS and HVAC must be designed with their own redundant systems.

Physical access security to the actual IDF and all equipment that enables access to the network must be secured and controlled. Likewise for all IDF equipment, as well as the access into that equipment. Vendor access to the data center must be restricted and monitored more carefully with all the converged environment equipment in central locations.

Regional offices are weak spots for many law firms. Because they are small, they are sometimes assumed to be relatively secure environments, thus allowing looser standards for physical security and access to data infrastructure equipment. This is a potentially costly assumption. Satellite offices need to be secured and access-controlled as solidly as any IDF in the home office.

Perimeter Defense

The first line of defense has traditionally been at the perimeter. External facing firewalls from such manufacturers as Cisco, Checkpoint, Juniper, etc. should be complemented with IDS (intrusion detection systems) for a more complete view of the security stance.

Remote phones using VoIP should be secured and encrypted with a VPN device. If the remote location will be hosting computers as well, then those locations should be forced to update their anti-virus software and definitions to firm standards. Additionally, any VLAN, logical segregations and IP address subnets should also be extended to the remote phones. A two-factor authentication for the VPN users is also recommended for extra security. And because VoIP is a subsystem of the network, additional perimeter defense should be added to VoIP systems, including VoIP-aware firewalls and SIP-aware safeguards.

Network-Level Security

At the network level, access to the internetworking equipment should be secured by RADIUS or TACACS+. A password policy should be implemented, and all patches relating to security in the firmware should be installed routinely. All configurations with dynamic protocols should be locked down, such as routing protocols, NTP and SNMP. These should have their security abilities enabled and access lists should be controlling the source and destinations of their interactions.

An IP address scheme should have VoIP systems logically segregated from the data infrastructure. This separation aids flexibility in Quality of Services (QoS), manageability and scalability, as well as helps protect networks from eavesdropping attacks. Ideally, this separation should extend to all VoIP sub-systems. Each should be deployed on separate private IP networks and these should be non-routable RFC 1918 address range, according to the Defense Department's Field Operations VoIP STIG ("Voice over Internet Protocol Security Technical Implementation Guide").

More Security Recommendations

One element that many firms overlook when deploying VoIP is VLAN segregation and tagging the voice VLAN behind the data VLAN to prevent eavesdropping and to mitigate the vulnerability of the voice VLAN. This is considered a best practice and is recommended by security experts.

Since VLANs are separate collision domains, additional defense is provided against DoS (denial of service) attacks, packet sniffing, and viruses and other types of malicious code from spreading from one endpoint throughout the network. This also enhances performance, as the VLAN segregation reduces the collision domain and provides separation between potentially chatty applications that exists on the data networks.

To further enhance the VLAN separation and prevent potential VLAN hopping issues, ACLs (access control lists) or filters can be set up on the switches to restrict visibility and VLAN access from other VLANs.

Endpoints, like softphones, must be carefully reviewed as to how they will connect to VoIP servers. If the VLAN segregation and logical IP address separation is in place, a softphone can connect with VoIP components through a routed point either on the core switches or through a network card for a VoIP server on the data network. Either way they add additional points for security to be positioned. These security concerns should extend to WAN and remote access.

System-Level Security and Defense

At the system level, two excellent lines of defense are an effective username/password policy and regular installation of security patches and updates. Management access to the systems should be secured and encrypted to prevent unauthorized access to the management systems and consoles.

Application-Level Security and Defense

In addition to system-level security, VoIP-specific items such as voice mail systems, wireless VoIP and VoIP management have operated in an environment where the security was based mainly on physical security. These tools and forms of access now can travel across an IP network, and their security must be enhanced by reducing the access to these devices from the general network. The best protection is to confine them to a secured VLAN, using VPN or other secured methods.

Data Security and Defense

Data security must also be extended to dial plans, which can include home numbers and mobile numbers belonging to everyone in the firm. The same holds true for voice mail and e-mail messages via VoIP, because voice and data can be intercepted, recorded and stored without the knowledge or consent of the users.

The potential liabilities and issues that can arise from such threats are immense. Security considerations must be taken seriously and risks mitigated in the most efficient manner.

VoIP Security — the Bottom Line

The features and benefits of VoIP communications are many, and the lure to roll it out in fast-moving, forward-looking organizations may be tempting. But when thinking about doing so, firms should carefully consider the security ramifications. Making the right calls on security upfront will mean feeling more secure about VoIP in your firm.

VoIP now appears on the SANS Institute Top 20 Internet Security Targets, a consensus list of top vulnerabilities for 2006 compiled by experts in the field, sobering recognition that VoIP has become a serious target for hackers.

by Donna Payne of Payne Consulting Group



:: Is Your Metadata Showing?

Within legal circles, metadata is a ubiquitous term, frequently discussed in journal articles, seminars and IT briefings. Even so, many legal professionals do not understand what metadata is and how it works. Simply stated, metadata is hidden information stored within a document, an electronic “fingerprint” that automatically adds identifying characteristics such as the creator or author of the file, the name of individuals who have accessed or edited the file, the location from which the file was accessed and the amount of time spent editing the file. In addition to data that is automatically added to a document, there is also user-introduced metadata, such as tracked changes, versions, hidden text and embedded objects.

This article focuses primarily on metadata contained in Microsoft Word files. However, metadata also exists in other commonly used word processing programs such as Corel WordPerfect, as well as in other types of programs including Microsoft Excel and PowerPoint.

This article examines metadata types and provides information on how legal professionals can eliminate metadata to prevent common pitfalls. Also covered are recent cases, rulings and opinions that are related to metadata. However, it does not attempt to explore the ethical implications related to removal of metadata from documents.¹

How Metadata Is Added

Metadata is automatically added to a file when the file is first created and then saved. It is also added when a user opens and edits the document. For instance, when a new document is created, associated Create Date and Author Name metadata are added. Likewise, when a file is printed, the document is tagged with a Printed Date.

Other metadata tags are also added, such as which template was used to create the document and the original author of the template. In addition, there is metadata denoting the full name and path of where the document was stored for the last ten authors of the file. If a template and macro package for document creation or a document management system as a document repository is used, more metadata will be added to the file.

File Properties Dialog Box

The most basic metadata is available through via File>File Properties. Individuals whose firms use a document management system may not be able to access this dialog box; however, recipients of the document outside the firm can, so it's important to know what information is traveling with the file. Following is a list of metadata that is stored in the File Properties dialog box:

Version of the software used to create the file

Full name and file path where the document is located on the computer or network

File size

Dates, including when created, last modified and last printed

Summary information such as the title of the document, subject, author, manager, company name, category, keywords, comments, hyperlinks, and which template was used to create the document

Name of the person who last saved the document, the number of revisions made, and the total amount of time spent editing the document

Custom properties that may be added to the document, such as the document identification number (client/matter) or a trail of e-mail recipients, along with the subject of the e-mail message to which the document was sent as an attachment (if e-mail properties are enabled).

Accessing the File Properties Dialog Box

To view metadata in your own document:

1. Open the file.
2. Select File>Properties.
3. Navigate through the General, Summary, Statistics, Content, and Custom tabs to view properties of the document. Remember that if you use a document management system, you may not have access to this dialog box.

User-Introduced Metadata

The properties of the file represent only a portion of the metadata stored in documents, but exemplify how metadata automatically is added to a file without the knowledge of the end user. Other metadata is added through the Field, Track Changes and Versions features.

Field Feature: Individuals without access to the File Properties dialog box (due to their firm's use of a document management system) may find it helpful to use the Field feature. Like File Properties, the Field feature can be used to view the total amount of time users have spent editing a document. (See "Using the Field Feature.") Many other fields can display metadata or hidden information, as well. For instance, individuals can ascertain the author of the document by inserting the author field and the date the document was created by inserting the CreateDate field.

Using the Field Feature

Using the Field feature is one way to find out the total amount of time users have spent editing a document. Here's how:

1. Open a document that previously was saved.
2. From the Insert menu, choose Field.
3. Under Categories, select All from the drop-down menu.
4. Under Field names, select EditTime.
5. Under Format, select the 1,2,3, ... option.
6. Click OK. The amount of time in minutes a document has been open will appear in the document.

Track Changes Feature: The ability to track all document changes is available in most word processing programs. When reviewing contracts, it is common practice to hide the changes and show the document in final format or as a final version. However, what happens if an attorney forgets he or she has hidden the tracked changes and sends the document to opposing counsel? The result is accidental disclosure with the potential for an unmitigated disaster.

Versions Feature: When this feature is enabled, a subset of the document, all changes, the author of the changes and the date and time the changes were made are saved in a "micro" version of the document. This data is stored within the document without any visual indicator or warning that these previous versions reside in the same document. To access Versions, select File>Versions.

Recent High-Profile Exposures

There have been many high-profile documents exposed as having metadata. For example, in 2005, the United Nations released a report on Syria's suspected involvement in the assassination of Rafik Hariri, Lebanon's former prime minister. Track changes were enabled in the document, and the recipients of the file were able to view names that had been deleted from the document of people said to be involved in the assassination.²

Metadata discovery was essential in the trial of Merck & Co. and the litigation involving the painkiller Vioxx™.³ Through tracked changes that were accidentally left in a document and later discovered by the *New England Journal of Medicine*, it could be asserted that the manufacturer knew of the potential heart problem side effects two years before marketing the drug.⁴

Using Track Changes

Enabling the Track Changes Feature

If you would like MS Word to keep track of revisions you make to a document, you will need to enable the Track Changes feature. Here's how:

~MS Word 97 or 2000: From the Tools menu, choose "Track Changes" and check the option "Track Changes While Editing."

~MS Word 2002 (Office XP) or 2003: From the Tools menu, choose "Track Changes."

Displaying Other Users' Changes

If you receive a document that has been worked on with the Track Changes feature enabled, but you don't see any of the changes or revision marks, you will need to instruct MS Word to display these changes. Once displayed, you can accept or reject them. Here's how:

~MS Word 97 or Word 2000: From the Tools menu, select "Track Changes," and then "Highlight Changes." Check the "Highlight Changes on Screen" option, and then select the "OK" button. To accept or reject changes, from the Tools menu, select "Track Changes" and then "Accept or Reject Changes." Use the "Find" button to navigate through all existing changes in the document, or select the "Accept All" or "Reject All" buttons to affect the changes throughout the document at once.

~MS Word 2002 or 2003: From the View menu, choose "Toolbars," and then select the "Reviewing" option. The first option on the Reviewing toolbar is the Display for Review drop-down menu. From this menu, select "Final Showing Markup." The Reviewing toolbar also contains "Accept Change" (look for the blue checkmark) or "Reject Change/Delete Comment" (look for the red "x") buttons. These buttons can be used to accept or reject individual changes in a document, or to globally accept or reject all the tracked changes in a document.

What Do the Courts Say?

One of the more detailed opinions on metadata was written about the age discrimination/reduction in force (RIF) in *Williams v. Sprint/United Management Company*,⁵ where discovery requests included the native electronic copy of the Excel workbook and its associated metadata. The presiding judge declared that the requested documents should be supplied with the metadata intact, unless both parties agreed that the metadata is not relevant or the producing party requests a protective order. This is significant because it meant that the calculations used to derive the information in the spreadsheet were considered to be metadata relevant to the case.

In the Priceline.com securities class action,⁶ the court ruled that the defendants could use PDF or TIFF file formats for discovery purposes, provided that they also supply searchable metadata databases and maintain all files in their native software application, with metadata intact, for the duration of the litigation.

These cases and others like them clearly demonstrate that legal professionals must remain vigilant about metadata in documents. Two documents that attempt to define the discoverability of electronic documents and metadata are the Federal Rules of Civil Procedure⁷ and the Sedona Guidelines.⁸ The Sedona Guidelines were published in September 2004 by the Sedona Conference, an organization composed of judges, lawyers and scholars.

As metadata and electronic discovery become more prevalent in the courts and in case law, more rules are being added to codify the practice

of electronic discovery. Recently, the Supreme Court approved e-discovery amendments to the Federal Rules of Civil Procedure, which went into effect in December 2006.⁹ Most notable with respect to metadata, amendment 26(a)(1)(B) substitutes the words “electronically stored information” for “data compilations” as a category for the required initial disclosures.

Rule 26 amendments also cover the exclusions of parties from providing discovery of electronically stored information when the provision of this information is not reasonable because of undue burden or cost; however, the burden remains on the producing party to make the required showing. Rule 34(a) is amended to reference electronically stored information and 34(b) accords parties the right to specify the form or forms of production for electronically stored information sought in discovery.

As more cases involving discovery of electronic documents and metadata are decided by the courts, more rules will undoubtedly be adopted to clarify the role of metadata in discovery.

Two states, New York and Florida, have already addressed the ethics of searching documents received from opposing counsel or in discovery for metadata, so-called metadata mining. Both have expressly declared the practice unethical.

New York State Bar Opinion 782¹⁰ states, “Lawyers must exercise reasonable care to prevent the disclosure of confidences and secrets contained in ‘metadata’ in documents they transmit electronically to opposing counsel or other third parties.”¹¹ The opinion goes on to say, “Lawyer-recipients also have an obligation not to exploit an inadvertent or unauthorized transmission of client confidences or secrets.”¹²

N.Y. State Opinion 749 (2003) concludes that:

The circumstances of the present inquiry present an even more compelling case against surreptitious acquisition and use of confidential or privileged information than that presented by the “inadvertent” or “unauthorized” disclosure decisions. First, to the extent that the other lawyer has “disclosed,” it is an unknowing and unwilling, rather than inadvertent or careless, disclosure. In the “inadvertent” and “unauthorized” disclosure decisions, the public policy interest in encouraging more careful conduct had to be balanced against the public policy in favor of confidentiality. No such balance need be struck here because it is a deliberate act by the receiving lawyer, not carelessness on the part of the sending lawyer that would lead to the disclosure of client confidences and secrets.

Nor need we balance the protection of confidentiality against the principles of zealous representation expressed in Canon 7. Our Code carefully circumscribes factual and legal representations a lawyer can make, people a lawyer may contact, and actions a lawyer can take on behalf of a client. Prohibiting the intentional use of computer technology to surreptitiously obtain privileged or otherwise confidential information is entirely consistent with these ethical restraints on uncontrolled advocacy.¹³

The Ethics Committee of the Florida Bar has issued a proposed advisory opinion that directs lawyers to take reasonable steps to safeguard

metadata in documents and instructs lawyers who are recipients of documents to not purposefully view metadata that is not intended for the recipient.¹⁴ The proposed rule excludes metadata “that is discoverable under applicable rules or is admissible in a trial or arbitration.”¹⁵

The Problem with These Rules and Opinions

One difficulty with any hard and fast rule on metadata is proliferation of versions and software applications used throughout the legal community. In MS Word, versions of the software process, store and purge metadata differently. For instance, MS Word 97 stores more author information than later versions. MS Word 2002 and 2003 include options to automatically display residual tracked changes and comments when a file is opened or saved, thereby showing residual tracked changes through no deliberate action to seek out the hidden information. Unless all lawyers are on the same platform and version, the playing field is not level.

System security policies are also available to large firms who use automated installation packages such as the Custom Installation Wizard from Microsoft for configuration and software deployment. These tools only work with Enterprise versions of Microsoft Office and are not available to sole practitioners or firms that purchase the software through original equipment manufacturers. The policy templates also can be configured to control the amount of data that is gathered.

In the case of IT, unfortunately, size does matter. Small firms have fewer tools available to them and often lack the resources to hire a dedicated IT staff tasked with keeping the firm software up-to-date and compliant with technological demands.

How Attorneys Can Protect Themselves

The best way for attorneys to protect themselves is to know what metadata exists in their documents before sharing the documents electronically. For example, knowing whether the Track Changes feature has been enabled and whether there are any residual changes in the document is important. Both must be cleared to protect the attorney from accidental disclosure.

Attorneys also should ensure no other versions of the document are stored in the file. In MS Word, this is done by choosing File>Versions.

Finally, view the Properties dialog box to make sure no proprietary information is displayed. It may not be possible to remove all of the built-in file properties; however, individuals should get into the habit of checking this information. “Title,” “author” and custom properties are added to a document automatically and may contain outdated information or data that should not be disclosed to an outside party.

Microsoft Office XP and 2003 for Windows offer an additional security measure for removing metadata. To access this feature in MS Word, select Tools>Options>Security. Next, select the box next to the Remove Personal Information From File Properties on Save option. This action is document-specific, which means it needs to be re-selected for every document, unless the user deploys a third-party solution that automatically does this. Being aware of and using these options is a good starting point; however, they fall far short of what is necessary and only deal with a fraction of the total metadata that resides within each file.

Is PDF Safe?

With any electronic file transfer, it is critical to know what is in the file and take precautions to remove any confidential data prior to distribution. Documents that have been properly scrutinized and “sanitized” before being converted into PDF files will not expose redacted information.

The U.S. National Security Agency released a guide to removing metadata from MS Word and PDF documents.¹⁶ It explains proper and improper redaction techniques and the preferred method for preparing and distributing sensitive documents.

Redaction software should be used to obfuscate material that is not intended for general viewing. Another effective method for redaction is printing a hard copy of the file, marking it up and then scanning the document to create the electronic file. It may sound “old-school” to some, but it ensures that information not meant for general viewing is not disclosed. It is imperative for legal professionals to understand applicable court rules before altering any original document. Some redaction tools create a new document; thus, violating some court requirements that metadata remain with the document and only pre-agreed upon information is redacted.¹⁷

An Adobe Acrobat user can set additional options to protect PDF files from accidental disclosure. In particular, two options can be disabled that control the amount of metadata saved within the document. Select Adobe PDF from the menu bar within the word-processing application; choose Change Conversion Settings from the drop-down menu; and then uncheck the options Convert Document Information and Attach Source File to Adobe PDF.

Protection options that prohibit copying and pasting also can be set in Acrobat to further increase the effectiveness of the software. Just make sure to password-protect the file so that people who have Acrobat cannot change security settings.

Third-Party Metadata Removal Software

Deploying a third-party metadata removal tool is the attorney’s best line of defense in the fight against unwanted metadata. The tools that are available today offer varying levels of protection. Some are more effective than others. When comparing different products, look closely at what they offer as far as levels of analysis and removal. Check to see whether the tool offers additional protections and features such as PDF conversion, e-mail integration and customization to meet the needs of the office environment.

Additional Considerations for Addressing Metadata

Metadata often is considered “the smoking gun” in litigation, and there appears to be a more concerted effort to obtain it in discovery. It is equally important for sole practitioners, larger law firms and in-house counsel to be aware of their ethical obligation with respect to the removal of metadata and protection of attorney-client privileged information.

The first step toward accomplishing this is to create internal standards on how future incoming and outgoing documents should be handled. Also, it is productive to evaluate how historical files are introduced into the organization and create a retention policy. Technology can be put

into place to help secure confidential information and metadata removal and purchase additional software, if applicable.

Finally, it is imperative to keep up-to-date on opinions, ethical rules and cases involving metadata. Obtain a copy of the Sedona Guidelines¹⁸ on working with electronic documents along with the NSA document¹⁹ referenced in this article.

Lawyers also must also reflect on whether there is an obligation to warn clients of the issues associated with metadata. Some very basic questions that every attorney needs to ask include:

Do lawyers have a duty to warn clients of the metadata risk?

Do lawyers have any kind of duty, in zealously representing the interests of their clients, to look at the metadata in incoming documents?

If clients are warned, how do lawyers handle the public relations challenge of explaining why it has taken so long to bring this to light?

There are many considerations, but one thing is certain: Metadata is a component of most, if not all, software that produces electronic documents. And it’s one that no attorney can afford to ignore.

ENDNOTES

- 1 For a more in-depth article on metadata, see Zall, “Metadata: Hidden Information in Microsoft Word Documents and Its Ethical Implications,” 33 *The Colorado Lawyer* 53 (Oct. 2004).
- 2 Bone and Blanford, “UN office doctored report on murder of Hariri,” *The Times Online* (Oct. 22, 2005), available <http://www.timesonline.co.uk/article/0,,251-1837848,00.html>.
- 3 Langreth and Herper, “Merck’s Deleted Data,” *Forbes Magazine*, (Dec. 8, 2005), available at http://www.forbes.com/home/sciencesandmedicine/2005/12/08/merck-vioxx-lawsuits_cx_mh_1208vioxx.html.
- 4 *Id.*
- 5 *Williams v. Sprint/United Management Company*, 230 F.R.D. 640 (D.Kan. 2005).
- 6 *See In re Priceline.com, Inc., Sec Litig.*, No. 3:00CV01884 (DJS), 2005 U.S. Dist. LEXIS 33636 (D.Conn. Dec. 8, 2005).
- 7 *See Fed. R. Civ. P.* 34.
- 8 *Best Practice Guidelines & Commentary for Managing Information and Records in the Electronic Age*, available at http://www.thesedonaconference.org/content/miscFiles/publications_html?grp=wgs110.
- 9 For the text of the Federal Rules of Civil Procedure Amendments, *see* http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf.
- 10 *See* http://www.nysba.org/Content/NavigationMenu/Attorney_Resources/Ethics_Opinions/Committee_on_Professional_Ethics_Opinion_749.htm.
- 11 *Id.*
- 12 *Id.*
- 13 *Id.*
- 14 *See* <http://www.floridabar.org/tfb/TFBETOpin.nsf/basic+view/OA1B5E3A86DF495A8525714E005DD6FD?OpenDocument>.
- 15 *Id.*
- 16 National Security Agency, “Redacting With Confidence: How To Safely Publish Sanitized Reports Converted From Word to PDF,” (Dec. 2, 2006), available at <http://www.nsa.gov/snac/vtechrep/1333-TR-015R-2005.PDF>.
- 17 Payne Consulting Group currently offers a free Scramble and Redaction tool (<http://www.payneconsulting.com>) as does Microsoft (<http://www.microsoft.com>). Other paid products are available; however, most do not offer any more substantial benefit over the free utilities.
- 18 *Supra* note 8.
- 19 *See Fed. R. Civ. P.* 34.

::Managing the Menace of Metadata

by Randy Farrar of Esquire Innovations, Inc.

Some types of metadata have been used for years to identify, classify and manage documents in the legal environment. But even as electronic document exchange increases exponentially, and with it, awareness that most documents and files include hidden data, firm-wide understanding about metadata management as a real security concern still lags.

Lurking Risks of Metadata

At best, unintentional disclosure of confidential information can be awkward; at worst, it can raise the specter of malpractice. Potential metadata misuse scenarios include:

Using dup-and-revise (Save As) to create new documents. When Microsoft Office documents are repurposed, the original author information, document properties, document variables and last print date usually stay with the document. Hidden text is often forgotten and carried over. Most authors are not aware that much of this metadata can be seen by looking at the document properties or by opening the document using a text editor or metadata viewer.

Applying track changes as a collaboration tool. When a document has been reviewed using track changes, the marked edits can still remain with the document — even if they are not visible to the eye — unless those changes have been accepted. The track changes feature can be turned off, but this does not eliminate the markings. Turning the display back on will reveal any revisions that have not been accepted and incorporated into the document.

Inserting comments to add a private note or annotation. As with track changes, comments created in Microsoft Office applications remain with a file unless deleted. Once comments are inserted, the comment display may be turned off. Any recipient of a document containing comments that are merely hidden can redisplay them easily. This may reveal confidential or potentially embarrassing information never intended to be viewed by anyone outside of the originating company.

Adding “identifier metadata” to your documents. Certain kinds of metadata can reveal the originator of the document based on the information’s uniqueness to both the user and firm. Identifier metadata includes uniquely named styles, bookmarks, hidden document variables and built-in custom document properties. Identifier metadata, though not necessarily high risk, should be managed if the originator needs to remain anonymous or if document creation strategy might be revealed by the metadata trail.

Key Strategies for Metadata Control

As the legal community becomes increasingly aware of the damage unintentional disclosure of document information can cause, the necessity for establishing metadata control strategies and parameters becomes blatantly evident. These include:

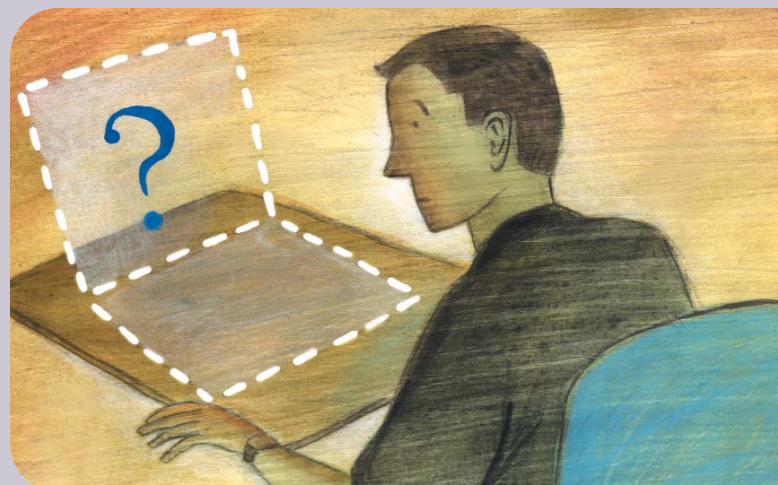
Educating your firm about metadata concerns. Attorneys and support staff who prepare documents should be made aware of what software features may embed metadata (e.g., track changes, comments, document properties), as well as the ramifications of using them. Much of the metadata inherited from the practice of repurposing documents can be eliminated simply by using templates containing minimal metadata.

Controlling and managing metadata with third-party metadata scrubbing and management software. Microsoft provides a basic metadata removal tool for Microsoft Word. More powerful third-party applications not only scrub metadata but also allow firms to manage it at a very detailed level.

Establishing a firm-wide metadata scrubbing and management policy. Implementing metadata-related policies and procedures can eliminate the need for individual users to decide what metadata gets scrubbed, resulting in a more efficient and standardized scrubbing process. Key users, especially attorneys, should be involved in any decisions about what is automatically removed and what is optional.

Use the Tools!

Data about the data can be as important as the data itself — possibly even more so in some cases. So seriously consider availing yourself of these and other tools and strategies. They are readily available and can mitigate the risk of metadata misuse.





by Faith M. Heikkila of Pivot Group

:: The New E-Discovery Rules

Take the Lead in Ensuring Compliance

New rules for electronic discovery adopted as part of the Federal Rules of Civil Procedure (FRCP) went into effect December 1, 2006. The purpose of these rules is to streamline e-discovery requests. In an attempt to minimize the number of motions to compel discovery, the federal courts have mandated discussions of how document production will proceed and what form the responses will take prior to issuance of its scheduling order. As a result, parties to a case now have an obligation to find out where data resides on their own systems in anticipation of any discovery requests.

As part of the information technology team, you can look forward to fielding questions and requests from your litigation practice group as to electronically stored information (ESI) formats that exist within your firm and within your clients' systems.

The new e-discovery rules will be subject to interpretation by the federal courts. However, it is no longer an option to avoid discussing ESI with opposing parties. The new rules mandate that attorneys know their clients' document management systems and storage practices. If the attorney does not identify specific ESI to be expensive to produce and identify them at the beginning of the case, the court may order these inaccessible documents to be produced at the expense of the producing party. This may lead to an expensive judgment against the client and potentially a malpractice lawsuit filed by the client against the attorney.

Impetus of the New E-Discovery Rules

The new rules stem from recent opinions, starting with the Laura Zubulake's gender discrimination and retaliation case (*Zubulake v. UBS Warburg, LLC*) against her former bank employer. In one of five decisions, the court shifted the cost of discovery to Zubulake for retrieval of the data from backup tapes (*ZUBULAKE I*). However, when the judge later opined that the bank had failed to preserve electronic

evidence and instructed the jury to assume the lost e-mail messages would be unfavorable to the bank, the cost for this production was charged back to the bank (*ZUBULAKE V*). In April 2005, the jury found for Zubulake, and she was awarded \$29.3 million in damages primarily because the bank had failed to adequately preserve evidence.

The case of *Coleman v. Morgan Stanley* (2005 WL 679071), however, caught the attention of law firms. In this case, the jury awarded in excess of \$1 billion to the plaintiff based on the mishandling of backup tapes by Morgan Stanley and their counsel. The court held that Morgan Stanley had been stonewalling and attempting to hide their e-mail, thereby violating numerous discovery orders (March 1, 2005 Order).

In the court's order, Morgan Stanley's attorneys were blamed for not having adequate knowledge about the ESI of their client. Thus, the new e-discovery rules provide motivation for communicating with clients' IT personnel at the early stages of the case to discuss data (evidence) preservation, the types of ESI under the client's control, whether the data is accessible and inaccessible, and the costs associated with producing inaccessible ESI.

What Are the New Rules?

The new e-discovery rule changes are included in FRCP 16, 26, 33, 34, 37, and 45. The Amendments to FRCP 33, 34, and 45, provision the addition of ESI to the rule. The following are the more extensive Civil Rule changes:

Rule 16 Pretrial Conferences; Scheduling; Management (b) Scheduling and Planning

Rule 16 (b)(5): "The scheduling order may also include provisions for disclosure or discovery of electronically stored information;"

Rule 16(b)(6): “The scheduling order may also include any agreements the parties reach for asserting claims of privilege or of protection as trial-preparation material after production;”

Due to the pervasiveness of computing and the current trend to produce documents in native electronic format, the amendments attempt to encompass all ESI and delete the previously used term “data compilations” in order to more accurately state the proliferation of electronic documents in various formats.

In the past, paper productions during the discovery phase included a privilege review of the documents prior to production. With the abundance of metadata and other versions of the data included in native file formats, data will be produced that is not visible and may include privileged information.

The attorneys may stipulate to a non-waiver of privilege agreement with regard to this type of inadvertent disclosure of privileged information. Obviously, it would be more beneficial to know upfront what types of data could possibly contain metadata and how to remove it prior to production in a good faith effort to perform a pre-production privilege review. Thus, the court acknowledges by way of Rule 16(b)(6) that there may be some inadvertent disclosure of privileged documents due to the nature of ESI.

Highlights - Rule 16(b) Amendments: The scheduling order may include an agreement crafted by the attorneys of record covering how inadvertent disclosure of privileged information will be handled when discovered after production.

Rule 26 General Provisions Governing Discovery: Duty of Disclosure

Rule 26(b)(2)(B): “A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.”

Rule 26(b)(5)(B): “Information Produced. If information is produced in discovery that is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has and may not use or disclose the information until the claim is resolved. A receiving party may promptly present the information to the court under seal for a determination of the claim. If the receiving party disclosed the information before being notified, it must take reasonable steps to retrieve it. The producing party must preserve the information until the claim is resolved.”

Rule 26(f): “. . . the parties must, as soon as practicable and in any event at least 21 days before a scheduling conference is held or

a scheduling order is due under Rule 16(b), confer to consider the nature and basis of their claims and defenses. . . .”

Rule 26(f)(3): “any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced;”

Rule 26(f)(4): “any issues relating to claims of privilege or protection as trial-preparation material, including — if the parties agree on a procedure to assert such claims after production — whether to ask the court to include their agreement in an order.”

With the propagation of inexpensive storage devices, your client could feasibly have terabytes of data to be considered in an e-discovery response. Aside from the typical locations for storing data such as network servers, hard drives, shared drives, laptops, and backup tapes, there are many others to consider as well. These include mirroring of data on redundant systems, instant messaging, file transfers using instant messaging, CDs/DVDs, smart phones, cell phones, BlackBerry devices, Palm Pilots, other personal digital assistants, MP3s, and thumb drives.

The attorney may come to you for assistance in figuring out what sources will be most difficult to produce in collaboration with the client’s IT person. From this information, the parties will develop a list of ESI that may be difficult and cost prohibitive to retrieve. This resultant document may also clarify to your client the costs associated with requesting unduly burdensome data and assist with the decision as to whether or not they want to pay for the production of these documents.

During the early 1990’s, it was no picnic to review millions of responsive documents for attorney-client and/or work-product doctrine privilege one page at a time. As a result of the explosion of ESI, more reviews began to include the use of software capable of assisting in searching for such documents during the privilege review. More document production requests now ask for documents in their native file formats, especially e-mail messages. The privilege review has once again become more onerous since there is metadata contained under the surface of what can be seen on the computer screen. Due to the presence of underlying information embedded in the ESI, there is a high likelihood that privileged information will be produced to opposing counsel unknowingly.

Highlights - Rule 26(b) Amendments: The attorneys need to know the location(s) of their clients’ responsive ESI as well as what the economic impact of paying for the production of inaccessible documents will be for their client. The court is forcing a proactive review by determining upfront whether the case merits the expense of retrieving inaccessible ESI. The anticipated result will be a more narrowly defined set of document production requests. Clients will have to decide at the start of a case whether they are willing to pay for the restoration of inaccessible ESI.

Pursuant to the amendments to Rule 26(f), the parties are required to meet and confer at least 21 days before a scheduling conference to iron out any issues relating to the discovery of ESI. This is the rule that requires the form(s) in which the ESI will be produced to be included in the meet and confer report to the court. Parties to a federal court case

can no longer avoid considering ESI document requests. They have an obligation to find out where the data resides. In order to know what information would be overly burdensome and costly to produce, the client has to be aware of the various forms of responsive data to the document request. The attorney will serve as the advisor on what types of documents are responsive. You will have to inform the attorney as to the possible file formats and locations of such data. Your expertise will verify that the client's IT staff performs their due diligence.

Highlights - Rule 26(f) Amendments: The opposing parties must now meet and confer at least 21 days prior to the Rule 16(b) scheduling hearing to outline the ESI production form(s). During this meet and confer conference, the parties must also resolve how inadvertent disclosure of privileged information will be handled. This is a much earlier deadline for identifying responsive documents than how discovery was handled in the past and must be approached as soon as the dispute arises.

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

Rule 37(f): “Electronically Stored Information. Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.”

While there is still a statutory duty to preserve evidence, Rule 37(f) provides a “safe harbor” against spoliation in the event that data is deleted or written over in accordance with a routine business practice such as archiving/deleting e-mail messages after a set amount of days or the overwriting of previously deleted files. The Advisory Committee on Civil Rules acknowledges that ESI is dynamic and if separated from its system may be incomprehensible (Rosenthal, 2005). However, if there is a reasonable expectation that a lawsuit may one day be filed against the company, preservation of evidence practices should immediately go into effect. The attorney will handle instructing the client to put a litigation hold on potential evidence related to a case. It would be extremely helpful for the attorney to have an internal law firm IT person assist in educating the client. An independent audit of the system can also assist with the due diligence requirement of locating and identifying data file formats susceptible to modification and deletion.

Highlights - Rule 37(f) Amendments: The Advisory Committee recognizes that computing is dynamic and there may be inadvertent rather than intentional modification or deletion of responsive files. However, the ESI lost must be based on good-faith routine practices and not due to lack of placing a litigation hold on the responsive ESI collection.

How Can I Prepare to Help?

Microsoft prepared comments on the e-discovery rule changes during the public comment proceedings. In its request to appear, Microsoft filed a very extensive informative document which can be found at <http://www.uscourts.gov/rules/e-discovery/04-CV-001.pdf> detailing the history of computers and how they work. This document may serve as an educational resource for attorneys grappling with understanding how

data is stored (Southerland, 2006). It delineates some of the concerns of identifying and preparing a discovery plan early in the proceedings.

The task at hand is for you to assist the attorney in preparing for the “meet and confer” conference. Some considerations and investigation are merited when assisting in this regard:

Inform/Educate Attorneys and Clients: Prepare to be inundated with requests to attend meetings with the client's IT staff to figure out what ESI would be responsive to a document production for the meet and confer with opposing counsel. The critical agenda is to identify the ESI formats that would be extremely burdensome and costly to produce, such as backup tapes.

Therefore, prepare to discuss the retrieval mechanisms with the client's IT staff and be knowledgeable about what vendors may be of assistance in this type of production. There must be convincing evidence that the production of these types of ESI would be overly burdensome. If the magnitude of procedures needed to extract the ESI is not compelling, the federal judge may order the information be produced with the burden of the cost to be absorbed by the producing party.

Visio Network Diagram: “A picture paints a thousand words.” Become familiar with a program that will produce a network diagram showing where the data resides. This document will be extremely beneficial as an exhibit to the meet and confer report filed for the scheduling conference. Perform a network assessment to produce a network architecture diagram illustrating where data resides.

Technological Attributes to Discuss: The following table represents a small number of possible file formats your clients may utilize on their systems that can be included in the meet and confer report:

SOFTWARE	FILE FORMATS
MS Outlook and Outlook Express	.pst, .dbx, .mbx, .idx, .nch
MS Word	.doc
MS Access	.mdb
MS Excel	.xls
MS FrontPage	.html, .htm
MS PowerPoint	.ppt
MS Visio	.vsd
Novell GroupWise	.mlm
Netscape Mail	.na2, .smn
Photoshop	.jpg, .tif, .bmp, .psd
Audio software	.mpeg, .wav, .asf, .wma, .avi, .midi, .aiff, .au, .aac

Discover the Client's Policies & Procedures: As previously stated, the proliferation of inexpensive storage devices has spurred the belief that everything and anything should be saved forever “just in case I need it.” The consequence is an unmanageable system and more data than you could ever get your hands around.

When a lawsuit is filed against your client, or for that matter, your law firm, how do you respond accurately? Without a records retention policy outlining the routine day-to-day operations in the normal course of business, deletions of data may be seen as destruction of evidence, and you can rest assured that opposing counsel will be quick to suggest a

sinister motive. A stop on all backups overwriting other files relevant to the case must be quickly implemented upon receiving a complaint in order to avoid destruction of evidence claims. As exhibited in the Enron case, destroying evidence may lead to jail time. By having a records retention policy wherein the purging and deletion of data is routinely implemented, sanctions and penalties can be avoided.

Get Your Own House in Order: By working through the details of a document retention policy for your own law firm, you will be better equipped to discuss file formats and data locations in response to a lawsuit against the firm. Additionally, when a lawsuit is filed, there is an obligation to preserve the evidence. Hence, it is crucial to have an e-discovery policy in place that identifies what steps need to be taken in order to assure this preservation of evidence.

Education and Preparation Will Help Ensure Compliance

It's very important to distribute the Amendments to the FRCP Rules for e-discovery to the entire law firm IT staff and educate them on the importance and benefits to the firm. These amendments should be read in concert with the Advisory Committee on Civil Rules Notes, which will provide a more in-depth understanding of the spirit of these new rules.

In order to accurately describe and develop an e-discovery plan, it is crucial for attorneys to learn as much as they can from their own IT staff in order to effectively question their clients' IT personnel. As the federal courts interpret these new e-discovery rules, attorneys will have a clearer picture of what the court expects during the meet and confer conferences and the scheduling order hearing.

In the meantime, develop e-discovery policies and procedures that revolve around records management for both the clients and the law firm. Additionally, procure and implement the appropriate e-discovery technologies and training. Then, take action. Assess your e-discovery readiness by finding the responsive document locations and determining the costs associated with the recovery of inaccessible documents and performing a document location assessment. Finally, repeat the process by performing regular reviews of the e-discovery policies and procedures to ensure compliance and continuous improvements. If you take the lead in preparation, you can feel confident your firm and its clients will be ready to handle discovery requests appropriately.

References

Amendments to Civil Rule 16, 26, and 37 to the Federal Rules of Civil Procedure, Effective December 1, 2006, www.uscourts.gov/rules/EDiscovery_w_Notes.pdf.

Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., 2005 WL 679071 (Fla.Cir.Ct., Mar 01, 2005) (NO. 502003CA005045XXOCAI).

Rosenthal, L. H., (2005, July 25). Report of the civil rules advisory committee. *The New E-Discovery Rules*, 19-27, ISBN 0-9773729-2-8.

Southerland, C. (2006, July 25). Are litigators ready for the new meet-and-confer sessions? *Law.com*, www.law.com/jsp/newswire_article.jsp?id=1153818330035.

Zubulake v. UBS Warburg, LLC, 217 F.R.D. 309 (S.D.N.Y. 2003). ZUBULAKE I.

Zubulake v. UBS Warburg, LLC, No. 02 Civ. 1243, 2004 WL 1620866 (S.D.N.Y., July 20, 2004) ZUBULAKE V.



About the Authors

Carlos Batista is the Information Security Manager for Alston & Bird LLP. Carlos has over six years of IT management experience, most notably in security and network management. He holds a B.S. in Criminal Justice from Georgia State University and has numerous certifications, including the Certified Information Systems Security Professional (CISSP) and the Certified Information Security Manager (CISM). He can be reached at Carlos.Batista@alston.com.

Randy Farrar, President/CEO and Chief Software Architect at Esquire Innovations, Inc., has pioneered the development and marketing of several practice management software applications geared toward the legal market. His training background has given him a thorough working knowledge of the specific problems faced by the legal industry when it comes to document production. He has extensive knowledge of many Microsoft products and has been the project lead and developer on more than 100 legal migrations and upgrades. He can be reached at randy.farrar@esquireinc.com.

John Hall is the President of Integration Appliance (IntApp). He has presented at several industry events on topics including business process optimization, ethical walls enforcement, security management and new business intake. Prior to joining IntApp, John co-founded VA Linux Systems, where he spearheaded the creation of SourceForge.net, the world's largest open source development website, currently hosting over 100,000 application development projects and supporting over one million registered users. He can be reached at john.hall@intapp.com.

Faith M. Heikkila, Information Security Consultant for Pivot Group, is currently a Ph.D. Candidate in Information Systems at Nova Southeastern University, specializing in information assurance. She has over 18 years of paralegal and IT project management experience with two law firms in Michigan. All skill sets regarding information security risk management are within Faith's expertise and passion. She is a member of the Association for Computing Machinery (ACM), Association of Information Technology Professionals (AITP), Computer Security Institute (CSI), Institute of Electrical and Electronics Engineers, Inc. (IEEE), and Information Systems Security Association (ISSA). She can be reached at fheikkila@pivotgroup.net.

Atlas Lee is a Senior Consultant at eSentio Technologies and has extensive experience with business continuity planning. Atlas has over 23 years of IT experience, 18 of which are in the legal industry, with the past 16 focused specifically on business continuity planning. As the Director of Business Continuity at Shook Hardy & Bacon, he developed, managed and implemented all phases of the firm's business continuity strategy and information protection program. Atlas can be reached at Atlas.Lee@esentio.com.

Klaus Majewski is Product Marketing Manager at Stonesoft Corp. During the past three years, he has worked with Common Criteria, FIPS and ICISA certifications for Stonesoft products, and has done penetration testing and security audits based on ISO Standard 17799. Klaus has CISSP and CISA certificates, as well as a master's degree in computer science from Helsinki University of Technology. He can be reached at klaus.majewski@stonesoft.com.

Michael Oh is the founder and CEO of Heavy Water Ltd., based in New York, and has been in the technology field for more than 25 years. He founded the company in 1992 and has specialized in infrastructure engineering, architecture and security, and in the past few years has been involved in extensive VoIP implementations and security for the legal industry. Michael is widely recognized in the New York tri-state area as a leading expert in the field. He can be reached at moh@heavywaterltd.com.

Donna Payne is president of Payne Consulting Group, a development and training company specializing in law firms, corporate and government legal departments. She is a member of the Microsoft Legal Advisory Counsel, the American Bar Association, the American Society of Journalists and Authors and the Project Management Institute. Payne Consulting Group is creator of the Assistants: Metadata Assistant, Forms, Numbering, Recycle and Pleading. They have authored 12 books including the best selling series, *Word for Law Firms*. Donna can be reached at donnapayne@payneconsulting.com.

DISCLAIMER This report is designed for use as a general guide and is not intended to serve as a recommendation or to replace the advice of experienced professionals. If expert assistance is desired, the services of a competent professional should be sought. Neither ILTA nor any author or contributor shall have liability for any person's reliance on the content of or any errors or omissions in this publication.

COPYRIGHT NOTICE Copyright © ILTA 2006. All rights reserved. Printed in the United States of America. No part of this report may be reproduced in any manner or medium whatsoever without the prior written permission of ILTA. Published by ILTA. c/o Editor, 2450 Louisiana, Suite 400-616, Houston, Texas 77006