ALEXANDER MUENTZ

hardening your systems against litigation

Alexander Muentz is both a sysadmin (since 1999) and a lawyer (admitted to the bar in Pennsylvania and New Jersey). He'd love to be a hacker public defender but has to earn his living helping law firms do electronic discovery. When he's not lawgeeking, he tries to spend time with his wife and his motorcycle.
lex@successfulseasons.com

YOU SPEND ENOUGH TIME WORKING in IT, and you'll go to a conference. You get to see distant friends and colleagues, get free stuff, and maybe learn a thing or two. You come back with a headful of ideas. Sometimes a FUD-wielding salesperson actually gets you worried and convinces you that you need to fix something back home. There are times when it's justified, and other times when it's silly.

The lawyers who represent your organization are going to their own conferences, and there's a big scary thing on their radar. To make your life easier, I'm going to explain what they're worried about and how to prepare your systems for litigation. For brevity's sake, I'm lumping technology support roles such as system administration, network engineering, and user support into "IT." I'm both an IT professional and a lawyer, but don't take this as legal advice.

What's the big scary thing? Recent amendments to the Federal Rules of Civil Procedure (FRCP) [1] have changed what digitally stored information must be retained and turned over to other parties to a lawsuit. The FRCP are the ground rules for civil litigation in federal courts. Generally the largest and most complex lawsuits are heard in the federal system, and state court systems tend to look to the Federal Rules when they modify their own rules.

Substantial changes to the FRCP are rare, which is why there's lots of buzz right now. Every electronic discovery vendor is out there teaching Continuing Legal Education classes (CLEs) about what the new rules are, what they mean, the big scary sanctions, and why you should hire its firm to handle all the digital aspects of your lawsuit. I've been to a few of these CLEs and taught one of my own, so I can safely claim that other than forcing lawyers to sit down and read the rules over lunch, they're really not that useful, because no one knows what the rules truly mean yet.

A Quick Explanation of Judicial Review

Often rules and statutes are intentionally left vague to keep pace with changing social, economic, or technological conditions without having to revisit the basic law. To fill in the gaps in interpretation, judges look to previous decisions on similar facts, which may look to even earlier decisions. After a

few iterations of this process, whole new doctrines known as "judicial gloss" are created to answer any contingency. To fully understand the rule, often many judicial opinions must be read. This makes our law stable and predictable, but arcane to the nonlawyer.

There have been so few decisions on these rules that it's like trying to learn what's going to happen in a movie by watching the credits. Unfortunately for the lawyers, without judicial gloss to guide us, we can only guess at what they really mean, and that worries us.

And for good reason. Not only are the rules still open to wide interpretation, but getting it wrong can have serious consequences. For example, the FRCP now require that a party to a lawsuit make available any Electronically Stored Information (ESI) that is both "relevant to the claim or defense of any party" and is not privileged, cumulative, or "reasonably accessible due to undue burden or cost." Improperly withholding or destroying discoverable information can result in sanctions, either monetary or the exclusion of your side's favorable evidence. Until the women and men sitting on appeals courts start handing down opinions in a few years and giving us some more fleshed-out rules to follow, we will only make educated guesses to protect our clients. Adding to the anxiety is the generally low level of technological savvy among lawyers.

FRCP Affects Sysadmins and Other IT Professionals

The FRCP require parties in litigation, or to whom litigation is likely, to immediately preserve all information under their control that tends to support their claims or defenses in the lawsuit. Failing to preserve or intentionally destroying such information can result in sanctions. Once litigation is started, all parties must provide either a list of sources and locations of relevant information or the actual information to the other parties in a process known as *discovery*. Information, if delivered, must be provided either in the format originally used in the course of business or in a format agreeable to both sides. Parties can also request additional disclosures of relevant information and can attempt to force the other side to deliver information improperly held back. They can also require uninvolved parties to divulge relevant information under their control. Each side also has a duty to inform the other side if it locates additional relevant information.

Generally, there are few limitations on such disclosures. Information that is legally privileged, redundant, a trade secret, or classified can be withheld unless a judge orders its disclosure. Also, a party can claim that the information sought is "not reasonably accessible" due to effort or expense relative to the value of the lawsuit [2]. If the requesting side pushes the issue, it may get it but be forced to pay costs to make such information usable, such as for data recovery of damaged media, media or format conversion, or forensic analysis for deleted files.

Sanctions: The Scary Bits

What the lawyers are really worried about are discovery sanctions. Once litigation is foreseeable, intentionally or negligently destroying discoverable material can result in monetary or evidentiary sanctions. Monetary sanctions are normally limited to the legal bills expended in forcing the disclosure of discoverable information. Evidentiary sanctions can be uglier. Information improperly withheld may be barred from being used in court by the side that withheld it or may even result in loss of a claim or defense, which

can lead to losing the entire lawsuit [3]. There is a "safer harbor" provision in the FRCP that stipulates that any destruction of discoverable information resulting from the normal, automatic operations of your systems is not sanctionable. Right now that seems to be only relevant to operations with little user control—overwriting deleted files, rolling logs, and the like. Human-controlled but routine procedures such as tape rotation may not be covered here.

The Definition of "ESI" Is Open to Interpretation

The definition of ESI is intentionally vague, to incorporate any new technology, but 99% of e-discovery revolves around email and "edocs." Email is what you think it is, and edocs are the entire spectrum of end-user documents—MS Office files, CAD/CAM files, images, PDFs, and the like. Given the way in which most discovery is handled at large law firms, I like to call this the "presumption of printability." If the file can be printed, they're most likely interested in it, because that's what they're doing, in one form or another. IT-savvy firms are converting the files to .tiff and using an image database to host them for armies of lawyers to look at each email or document. But if it's something not immediately understandable to a human, such as a database file, or not printable, such as a sound or movie file, the big firms tend to set them aside unless they have a good reason to look at them.

Few lawyers get creative with their electronic discovery requests. I understand not wanting to demand all of the stored music or movie files on an opposing party's PC (unless you're the RIAA or MPAA), but many lawyers are resistant to requesting archived voicemails, IM chat transcripts, and the like. Every CLE that I've seen or taught on this issue has touched on the multitude of potential storage devices, including employees' home computers, mp3 players, thumb drives, PDAs, and cell phones.

ESI may even be information that isn't normally stored at all. A recent federal magistrate's decision in *Colombia Pictures v. Justin Bunnell*, commonly known as the Torrentspy ruling, upheld a litigant's request to force a Web site owner to keep and preserve requesting IP addresses when he originally did not store that information [4]. The responding side failed to prove that the logging would be unduly burdensome, as it was using Microsoft's IIS, which can easily log such information. Lots of people in this field are eagerly awaiting future rulings to see whether this rule is followed or ignored. Stay tuned.

How Lawyers Process This Information

A typical large litigation project works in stages. First, the lawyers determine what information is likely relevant to the litigation and which employees would have this information. They then collect it from their client and have armies of lawyers pore over it, both to get an understanding of the facts of the case and to mark any documents that may be excluded because of legal privilege, trade secret protection, or irrelevance. Once that is done, they start handing over this information to the other parties to the lawsuit and start looking at the information given to them by the other parties.

Where You Fit Into All This

Some background is useful to understand what the lawyers really want and need. You're important because most of this information is on systems that

you're responsible for. You or your group is most capable of collecting and preserving the data your organization needs. To assist, I'm going to give some suggestions of what you should be doing, depending on where your organization is in the litigation process.

STAGE 1: NORMAL OPERATION—NO FORESEEABLE LITIGATION

This is the time we like to think of as "project time." There are no major fires to put out, so you can think clearly about long-term fixes for issues such as litigation readiness. I'd recommend getting a handle on all the places where your organization stores data. Make an inventory of all your workstations and server shares, both active ones and the obsolete ones on the shelf. Figure out which users have or had regular access to what workstations, shares, databases, and other resources. If you've got some time and budget, look into archiving and indexing packages for email and end-user documents. If you support end users, look into remote control/login packages that allow you to collect locally stored data and email over a network.

Also, this is the time for you to work out your data retention and destruction policies. Work them out with everyone involved: the IT staff that implements and maintains it, as well as the legal and compliance crew that makes sure it's compatible with your legal and regulatory environment. Once you've got it all in place, stick to it. If something is supposed to be deleted, preserved, or destroyed, do so. Surprises during litigation aren't any fun.

For the desktop support crew, a decommissioning procedure, during which you index and archive the user files when a workstation or employee moves on, keeps you free from worrying about trying to find and resurrect obsolete machines a few years later. Doing the same for server shares that are no longer active also makes good sense. Having at least one working system that can read whatever media you chose to store those archives on will also make your lives easier, unless you like scouring eBay for antiques.

STAGE 2: REASONABLE LIKELIHOOD OF LITIGATION

A bunch of employees just jumped to your largest competitor, maybe with the products they were developing. Your organization is seriously considering suing someone. Ideally, your lawyers write up a nice, straightforward litigation hold memo and circulate it to the IT staff. Now your homework from Stage 1 pays off. With your list of shares, workstations, and users to preserve, all you need to do is keep the archives in a safe place, fire off a full backup of the current affected users, shares, and resources, and run incremental backups until the litigation hold is modified or ended. If you haven't prepared, you need to scramble. The legal department will need to send letters to all the affected users asking them to stop deleting relevant documents and email. You may get asked to enforce this, somehow.

STAGE 3: LITIGATION COMMENCES

Someone's filed suit. First off, the litigation hold may be modified and expanded. Second, you need to start putting all of your relevant ESI into two categories—easy and hard to produce. Your lawyers are going to want to know which ESI is expensive and time-consuming to hand over to the other side, in order to exclude it or force the other side to pay for the extraction. For each item you're preserving, come up with a rough estimate of the time and money it would cost. Be realistic: 4 GB of MS Office files in an end user's

home directory isn't going to take ten hours and a thousand dollars to produce, but that crate of 9-track isn't going to be cheap to convert into some modern, usable format, either.

Finally, you have to prepare for the "Rule 26" conference. FRCP 26(f) requires parties to sit down and work out a discovery plan. Included in such a plan is how to handle ESI: what format to give the discoverable information in, when to supply it, and where to deliver it. Each side should bring an IT professional who understands what information is sought, what format(s) it is in, and how difficult it would be to make it available to the other side in the format requested. This IT pro should also be able to explain technical concepts in simple, easy-to-understand language without getting frustrated.

If you haven't prepared for this during Stage 1, get ready for long nights and stress. I've worked a case where the client had no capability for remote archiving, so I had to travel to four separate cities to personally collect documents and email. If there had been old workstations or tapes that could have held discoverable information, I'd probably still be pulling data from them today.

STAGE 4: HANDING OVER DISCOVERY TO THE LAWYERS

The parties have started to agree on the scope of discovery, so you can go back to your archives and start pulling out information that complies with this. Now any indexing or searching capability you have is going to come in handy. The lawyers may have agreed to hand over any documents or email that contains a project name, or falls within certain dates, or to specific people. The ability to search and to limit the amount of discovery is going to reduce your legal bill, as the fewer documents your own lawyers have to review, the less billable time. In addition to the delivery of documents, there may be some assistance you can offer to the legal team in sorting and understanding the discovery that's going to start coming in from the other parties in the litigation. Having an IT person who knows the people and issues can only save money and reduce risk. If you can have one person as the "IT liaison," that person can coordinate among the rest of the IT department, the legal staff, and any consultants you may have hired to help, thereby reducing time, billable hours, and headaches.

Finally, there may be some additional modifications to the litigation hold memo. The IT staff should be prepared for last-minute changes, just in case.

In Closing

If you prepare for litigation like any other disaster, you're going to be far better off than if you crossed your fingers and hoped for the best. Knowing what you have, as well as what you don't, and having the ability to retrieve it cheaply and quickly will prevent headaches, save your organization money and time, and make you a hero to the nontechies.

REFERENCES

[1] Federal Rules of Civil Procedure (2006): http://www.law.cornell.edu/rules/frcp/.

[2] FRCP 26(b)(2)(b): http://www.law.cornell.edu/rules/frcp/Rule26.htm.

[3] FRCP 37(b)(2)(A),(B): http://www.law.cornell.edu/rules/frcp/Rule37.htm.

[4] *Colombia Pictures v. Justin Bunnell,* No. CV 06-01093 FMC (C.D. CAL 2007).