Preservation of ESI after Layoffs

Craig Ball

In a March 27, 2009 article in The National Law Journal called, “Protecting Corporate Data in Economic Downturn” authors Regina A. Jytyla and R. Jason Straight pose the question, "As work force cutbacks become commonplace, many organizations face the daunting task of locating, securing and imaging hard drives left behind by departing employees. For example, what should a corporation do with 30, 100 or even 1,000 idle computer terminals?" It's a great question. Unfortunately, the article ventured no answer.

Indeed, there's no pat response; but scant resources aren't a free pass to spoliation. Reductions-in-force are Alzheimer's to institutional memory. Suddenly, the people who know where responsive ESI lives and the ones caching stuff for litigation hold are gone. All that remains are their machines, file shares and a drawer full of little ketchup packages.

In-house and outside counsel must know how to react *molto pronto*. So, I write to put forward one low cost approach tailored to companies in crisis.

In performing preservation triage on dozens of idle machines, first undertake some mundane tasks, then make a couple of threshold decisions:

1. Label each machine and external hard drive or other storage media with the name of its former user, title, department and physical location and include relevant dates (e.g., terminated 3/31/09). If it's not a security issue, consider adding the custodian's username on that machine, along with his or her log in password and company e-mail address. Right now it's "Susan's machine," but soon it'll be just a chassis amidst a hundred others that look just like it. Be certain the labels are firmly affixed and applied in a consistent way so you can see them when the machines are stacked.

   Print two more copies of the label: one for the hard drive (see below) and the other to stick on the log sheet that will serve as a preliminary inventory record and ultimately input for your discovery database. Better still, generate the label data from a database holding the same information. Sure, you can use bar codes or RFID tags, if you want to go high tech. For my money, a prosaic paper label gets the job done for the lowest cost.

2. If a former user was subject to a litigation hold, create and prominently affix a warning label to that effect. You need to insure these machines don't get wiped, re-tasked or auctioned off until their contents have been harvested in all pending and anticipated matters, After that, you can put on a new label that says "okay to wipe" with someone's signature right on it for the sake of accountability. I keep a Brother P-Touch label printer attached to my machine because **mistakes are costly, and labels are cheap**.

3. While you're printing labels, affix some identical to those described above on the hard drives *inside* the machine. I like to include the serial number or service tag for the chassis on these labels. This small effort can save you big headaches down the line.

4. Secure the machines and external media. Even before a departing employee is out the door, co-workers start circling their office stuff like vultures over carrion. In no time, that stuff grows legs and walks off. Lock the machines up where they aren't likely to get wet, hot, frozen, stolen, borrowed, played with or cannibalized for parts.

5. Cell phones and other handheld devices pose unique challenges. Years ago, I was part of a group inspecting the Chicago ESI preservation facility used by Arthur Andersen in the Enron litigation. With an overweening air of "we know exactly what we're doing," Andersen's legal team pointed to shelves laden with carefully packaged desktops, laptops, hard drives and handhelds. I was duly impressed, but since handhelds of that era lost their data soon after batteries died, I asked what provision had been made to supply *power* to the trussed-up PDAs and phones during their weeks *en plastique*. The wild-eyed looks exchanged on the other side were answer enough. No deer ever faced headlights with greater dismay. A charging protocol was quickly implemented.

   Most handhelds spread data across three storage areas: the device's (sometimes volatile) memory, a removable media card and an online repository (e.g., a mobile service provider or a Blackberry Enterprise Server). If the device is synched with a computer, you have a fourth storage area to consider. Moreover, wireless devices keep interacting with the world--searching for signals, talking to towers and storing new data--if you don't intercede.

   Labels are your friend here, too. The user's name, title, department, messaging ID, account number, password and relevant dates. Consider adding a piece of tape to secure removable media too small to label. It's not rocket science, but it works.

6. Now, decide if any of the machines or devices are candidates for computer forensic preservation and examination. Unless the FBI is at the door or the New York Times has lately used the company's name in the same sentence with "Ponzi scheme," the need for wholesale forensic imaging is remote. However, firings often lead inexorably to litigation and, from fear or spite, departing employees engage in delete-o-thons before they go.

   On a shoestring budget, bring in forensics experts only if you have a reasonable basis to anticipate the need for forensic preservation and examination. For a list of situations where you *should* see the need, check out the *Ball in Your Court* column in the April 2009 issue of Law Technology News.

7. Sitting on dozens or hundreds of idle machines is a waste of resources, but so is collecting contents in anticipation of litigation that may never arise. Bankruptcy trustees, government overseers, even once-somnolent directors may insist that idle assets be put to work or converted to cash.

   How do you re-task or sell machines while meeting preservation duties?

   This is where it's helpful to consider computers separately from hard drives and ESI. Most people grasp the distinction between a DVD player, a DVD and a movie stored on DVD. A computer is like a DVD player, the hard drive is the DVD and the ESI on the drive is the movie: ***viewer, container and content.*** With one notable exception discussed below, it's possible to swap hard drives between machines and move ESI to new media.

   Strategy: Pull the drives, then re-task or sell the CPUs.

   "But wait, “you protest, "Doesn't much of the value of a computer flow from its operating system and all the software on the system?" Sure, but the software site licenses that companies buy from Microsoft and other software publishers don't allow them to sell the operating system or the software along with the hardware. Possessing an installed copy of a program is not the same as having a license to use it. Moreover, drives bound for the auction block or charity must be cleansed of confidential company data--something that's hard to achieve without devoting hours to wiping everything. Even re-tasking a system within a company involves some reconfiguration and/or re-installation of software.

The bottom line is that new drives are cheap, and *when an employee leaves the company and preservation is required*, trying to copy their drive or keep it in service ends up costing more than simply pulling, labeling and sequestering the drive. It's certainly a lot faster than duplication.

8. What kind of lawyer would I be if I didn't add, "but it depends?" The bonds between hard drive and machine are pretty weak to begin with (e.g., configuring the right drivers for the hardware) and of little consequence in e-discovery. In EDD, we rarely collect the system and application files that boot and run the operating system and programs. In fact, we de-NIST data sets to get rid of that stuff.

   But machine and drive are hopelessly conjoined in computers implementing the features of a **Trusted Platform Module** or **TPM**. Many newer laptops and some enterprise desktops sold today incorporate a TPM, though very few civilian users activate the full disk encryption and other features that prevent accessing data on a hard drive absent the TPM module used to encrypt the data. How few? Well, in the last 100 business laptops I've forensically imaged, not a single machine implemented TPM features.

   If the company deployed encrypted laptops keyed to the TPM, you're probably stuck keeping the whole machine ***and its password or USB activation key*** or collecting potentially responsive ESI from the drive while the user is logged in.

9. When you pull hard drives for preservation, don't forget those drive labels discussed above. Be sure the machine is powered off, and then pull the plug to be sure. It's a low voltage device, but why tempt fate?

   Some drives can come out in seconds without any tools. Others will require a Phillips screwdriver and some finesse. Don't cut yourself on sharp chassis edges. This downturn will pass, and your family needs you more than the employee death benefit.

   The mortal enemies of a hard drive are electrostatic discharge and rough handling. Touch a grounded surface (cold water pipe, grounded system chassis or freshly unearthed vampire) right before handling the drive. Handle the drive with care; which is to say hold it by its sides and don't drop it or squeeze hard on the drive enclosure. Affix the label somewhere that it won't just peel off, and try not to cover the parts of the drive's factory label detailing the size and serial number of the drive.

   Package drives to keep them clean and dry. Those specially-made, pink, antistatic bubble wrap bags are ideal; but a little low-static padding and a quart-size Ziploc freezer bag from the grocery store will do in a pinch. If the drives are individually well packaged, I find ordinary vinyl storage bins work well to store and protect as many as 20-30 drives in a secure room or closet.

10. Remember: ***The trick is not losing track of what you have***. Good labeling, careful inventories and making sure that multiple people--particularly the legal team--know what's where is key to this strategy.