

The Business Case for HDD Wiping

del.icio.us

Discuss in Forums {mos_smf_discuss:RichM}

This month's installment is inspired by all of the other tasks that require our attention which allows important things to slip through the cracks. What amounts to general laziness is really just a symptom of a much bigger problem: lack of time. As administrators we are expected to keep all machines (basically if it plugs into a wall, we should have encyclopedic knowledge about it) up to date, users should always be productive, oh and maintain a secure yet usable network. If that was the end it might be manageable, but of course there is always several "special" projects that require research, testing and most importantly time to implement. Therefore I understand when a menial task like formatting a hard drive doesn't get done, but I can't say that lack of time is a justifiable excuse.

Old hard drives are a rich source of unknown hidden treasures, even if they were only used by a temp or even a personal assistant. As is very common in corporate times, passwords are shared without much issue. If I had a nickel for each time I heard or watched a supervisor/Chief _____ Officer log into his assistant's machine, do some work, then log out, I would probably be writing this sitting in the sand under a palm tree.

In an effort to express the importance of sanitizing old hard drives, I present to you two scenarios, each with its own level of severity. Ultimately you have to decide if the extra effort is justified for the potential "what ifs" that are outlined below.

In the first scenario, we find the Chief Information Officer logging into his assistant's machine, browsing travel sites for an upcoming trip and logging out. Provided the executive didn't access shared drives or send email, I am not too concerned (other than the fact that, technically, password sharing violates my usage policy). One potential issue is if he were to log into the travel site with an account tied to a credit card number. That could potentially be a serious issue, and, depending on the limit of the card, very damaging. There isn't much that can be done about this. Since technically he can fire my boss, I have to acquiesce to the potential pitfalls brought on by his laziness.

The second scenario however goes a little something like this: The same executive's laptop battery dies. He is late for a budget meeting, so he does the work on his assistant's machine (logged in as himself). He doesn't save the file (creating an entry in the /tmp directory, under his profile), prints the spreadsheet (with a wealth of financial information) and powers off the machine. His assistant comes back from lunch installs a badly written .src file and Blue Screen's of Death (BLOD) her machine. She asks the help desk person on call for help, and they decide the best course of action is to replace the assistant's machine seeing it is an older model. All old files (mydocs, desktop, etc.) will be restored from backup. The hard drive is removed from the pc that houses it and is placed in a pile with dozens of other unlabeled hard drives where it remains for an extended period of time. Days fold into weeks, then months, and finally an admin decides its time for some spring cleaning.

A decision is made that IT resources are stretched too thin, and those once forgotten hard drives are now ear marked to be used for new hires which need a machine immediately. Since the need is so urgent, an executive decision is made that all hard drives will be formatted as part of the XP installation. As we all know this is a joke. There is a large amount of that data that can be retrieved for someone that is patient enough to harvest the information. I realize that many of you are reading this shaking your head, but I assure you it happens. In fact I have been instructed to do it on more than one occasion, and the hard drive in question had at least four profiles of users on it.

There are hundreds of ways in which information that doesn't belong somewhere can be found, and there is only one answer - clean those drives. If your organization has the money, hire a company that will degausse your drives. Or if you have really big pockets, pick one up for yourself. The current asking price about 10K. If you do not have that kind of money, but the hard drives are worthless to you, soak them in a bucket of water then have them properly recycled. If however the second scenario sounded all too familiar then your only option is to wipe the drive, but it must be done correctly to ensure corporate secrets stay secret.

The best application I have found for wiping hard drives is Darik's Boot and Nuke ("DBAN") at <http://dban.sourceforge.net/>. As always, I am not compensated by this manufacturer, it is just a tool I cannot live without, and know that it will give anyone (who has the patience) peace of mind. This is a freeware piece of software that can be downloaded to floppy or burnt as an ISO to disc. The program is self-booting and once you enter the 'autonuke' command, disc nuker will detect all hard drives present on the machine and write over all the data. It will take seven passes over the data and meet the requirements for the Department Of Defense (DoD) low-level formatting guidelines. However since it takes seven passes, it is somewhat time consuming.

If you have a large stack of old hard drives, your best bet is to create long chains of hard drives and run Dban overnight. If you set up several machines with multiple disc drives, the job shouldn't take that long. You will then have the peace of mind that, other than our government, no one can retrieve sensitive information that should be gone. This software will even run on a RAID 5 device, though it will take around 12 hours.

If you have the extra money, there is an enterprise-level sister product called Enterprise Boot And Nuke ("EBAN") at <http://www.techwayservices.com/eban-data-destruction/>. This product is efficient and will provide reports that can be used for accurate record keeping. I haven't looked into the price breakdown, but they claim it is economical and, if time is short, it could be a time saver that still allows for proper formatting of hard drives.

[Click for larger image of EBAN Screen Shot.](#)

I hope this quick look into hard drive wiping, albeit simplistic, still drives home the need for instituting policies and procedures for such actions in your own organization.