5-3-2012

Technical Bulletins: Disposing of a PC

Justin O'Hara
Municipal Technical Advisory Service, oharaj@utk.edu

THE UNIVERSITY of TENNESSEE
MUNICIPAL TECHNICAL ADVISORY SERVICE
...in cooperation with the Tennessee Municipal League

TECHNICAL bulletin

May 3, 2012

DISPOSING OF A PC

Justin O'Hara, Information Technology Consultant

Disposing of old computer hardware by auction or donation is a good way to get rid of older personal computers (PC) and provide them with a second life, which is also good for the environment. These are two noble ways to dispose of an old PC; however, something to keep in mind is that the hard drive on that PC could contain a treasure trove of information. A few examples of information that could reside on the hard drive are:

- Billing information;
- Credit/Debit Card Numbers;
- Driver License;
- Passwords; and
- Wireless Network Access Codes.

There are data thieves who purposefully mine places such as public auctions, flea markets and garage sales. These data thieves purchase old hard drives with the intent to find personal information to sell on the Internet. Not only do these thieves seek information on personally-owned equipment, they also look for public auctions of equipment such as PCs, printers, fax machines, copiers, etc. as all of this equipment contains hard drives and bits of electronic information that can be mined for profit.

According to the Tennessee disclosure statute (T.C.A. § 47-18-2107) releasing unencrypted personal information in this manner would most likely be considered a data breach. This, at the very least, would incur the notification section of the statute but could also go as far as a civil action against the information holder. In addition, the Fair and Accurate Credit Transactions Act (FACTA) contains a specific rule specifying the proper disposal of consumer information, which includes electronic records. FACTA also outlines penalties for "willful noncompliance" that also could include civil liability and punitive damages. Outside of what is required by law or statute it makes good cyber security sense to assure you do not have data left on an old PC.

For example, you have audited all your municipal PCs and know that you do not have any business processes that require you to gather and store consumer information, therefore not calling into effect either of the above instances. However, a PC might have an unencrypted file containing all of the user's passwords, compromising that user or wireless network settings and puts the municipality's wireless network security at risk, allowing someone access to municipal information technology (IT) resources.

A municipality should establish a written policy or procedure outlining the disposal process from start to finish, including methods of removing all data from existing PCs. The two options for removing the data from a hard disk are either a software tool to wipe (erase/overwrite) the data or physical destruction of the hard disk. Just deleting the files on the hard drive or reformatting and reloading the Operating System are not sufficient means to completely remove the data. If this has been your chosen method, the files can be recovered fairly easily.

May 3, 2012
DISPOSING OF A PC

A simple Internet search will help you find a number of good data recovery tools to retrieve files that have been deleted from the hard drive or other removable media. Some recovery tools will even work on drives that have been reformatted. I have used a few to recover photos and other files that have inadvertently been lost or deleted from PCs, memory cards, USB drives, etc. Most recovery tools have graphical user interfaces to make recovery as simple as possible. Most of the tools were not designed for nefarious reasons but could easily be used in such a manner. More sophisticated tools exist, but have a difficult time recovering data when using either of the data destruction methods discussed.

ESTABLISHING A WRITTEN PROCEDURE

Establishing a written procedure will help to assure everyone involved that the municipality has planned ahead and thought through the entire process of PC/data disposal. The plan should include the method of removing the data from all IT equipment so you can be assured that unencrypted data is not leaving your organization unintentionally. This policy should include a list of equipment that you know has or could potentially contain sensitive information. It could include copiers, faxes, servers, laptops, smart phones, desktops or basically anything that contains a disk drive (memory) and stores information. You would also want to outline the basic process for each device. For example, you could use the same process for all of the hard disk-based equipment, but you might have to use a different process for a smart phone. Next, you would outline the process you will use to auction or donate the equipment. This could include your method of selecting the receiving entity.

SOFTWARE DESTRUCTION

A couple of software tools for software destruction include DBAN (http://www.dban.org/) or Killdisk (http://www.killdisk.com/). DBAN is a free self-contained boot utility that securely wipes data from hard disks. Killdisk is very similar, but it is available in both a free/lite version and a paid/professional version. The professional version offers additional options for the type of wiping that is done on the drive. In both versions, you will download the .iso file from their website. The .iso file is a CD or DVD image file that you will need to burn to the appropriate media. Windows Vista and Windows 7 can do this natively, but Windows XP will need a third party utility such as Nero, Sonic or Ulead in order to burn the .iso file to CD/DVD. Once the .iso file has been burned to CD or DVD, you will then start from this CD/DVD on the PC containing the hard disk you would like to wipe.

(NOTE: This procedure cannot be reversed. Once you have started wiping the disk, you will no longer be able to retrieve the data.)

Both the DBAN and the free version of Killdisk can be used in a home/personal or business environment to completely remove data from an existing hard disk and render it very difficult, if not impossible, to recover. I would recommend Killdisk Professional for use in a municipal environment. DBAN does not disclose the method it uses to wipe the data and will not make a statement of conformity in removing data in compliance with Health Insurance Portability and Accountability Act (HIPAA), National Institute of Standards and Technology (NIST), Sarbanes-Oxley, etc. Killdisk, however, provides a basic statement as to the methods used to wipe a drive and allows you to choose the method

you prefer, as well as verifies (professional version) the data has been wiped.

The biggest advantage of the software method is that it does not destroy the hard disk. This allows the hard disk to be reformatted and the OS reinstalled afterward, allowing the computer to be set up and once again become a functioning computer.

PHYSICAL DESTRUCTION

The second method of purging the data is physical destruction of the hard disk. This can occur in many ways, including a sledge hammer, industrial shredders, degaussed, etc. However, with this method, you are destroying the media so the PC would have to be sold/auctioned/donated without a hard disk. Depending on the information that was stored on the hard disk, this may actually be the preferred method. For example, if you have lots of confidential information (names, addresses, credit card numbers or Social Security numbers), you may want to choose physical destruction. Some advantages of this method include ease of use, time (typically much faster) and convenience. The software method of wiping data removes the data and then writes a series of 1s, 0s and random characters to the entire surface of the disk. Killdisk Professional defines the US DOD 5220.22-M standard as three complete writes of data across the disk. Both free versions of the software tools only make a single pass across the disk, effectively taking one-third the amount of time. Depending on the number of writes that you choose and the size of the disk, you could be looking at hours or days with some of the larger 1TB drives. However, with a sledge hammer and the proper safety equipment, destruction can be handled in a short amount of time. Just remember to make sure the platters are in multiple pieces when you are done.

POLICY ASSISTANCE

If your city does not have an existing disposal policy that outlines the above process, MTAS information technology consultants can help you develop one to fit your organization.

MUNICIPAL TECHNICAL ADVISORY SERVICE

Knoxville (Headquarters) . . . (865) 974-0411
Jackson. . . . . (731) 423-3710
Johnson City . . . . . (423) 854-9882
Martin. . . . . (731) 881-7055
Nashville . . . . . (615) 532-6827

MTAS4390 • E14-1050-000-050-12