Global Information Assurance Certification Paper

Jason Youngquist
SANS Security Essentials
GSEC Practical Assignment Version 1.2e
Protection when you recycle your computer
September 27, 2001

Introduction

People need to protect the personal information on their computer, otherwise the results could be damaging. According to researchers at Carnegie Mellon University (The Business Review), the ratio of computers that are obsolete to those that are newly purchased is increasing. The ratio was formerly 2:3 but by 2005 the ratio is predicted to be 1:1. Instead of dumping outdated computers in landfills, government agencies and companies give them to schools and other non-profits. Non-profit companies receive obsolete computers from companies, repair them, and then give them to schools. Both the company and school benefit because the company gets a tax deduction and the schools get needed computer equipment. The refurbished computers may not be the fastest in the world, but are adequate to allow students to be engaged in the learning process.

Before individuals or companies donate computers to schools or other non-profits they first need to ensure that the computer does not contain any confidential information. The purpose of this paper is to describe some situations in which hard drives and other magnetic media were not erased properly. Four examples will be cited to illustrate how confidential information could be leaked to the general public and measures that can be taken to limit the release of confidential information.

Energy Department

The first case is from the United States government. In 1999, a division of the Energy Department in Savannah River was going to replace obsolete computers. The problem arose when confidential information was not removed from the hard drives. The computers were designated for China, but fortunately did not make it there. Luckily, the Department of Energy team did not find classified information on any of the computers or removable media, but this was the first time they reviewed this. Prior to this incident the Energy Department did not have a formalized policy to ensure that computers were sanitized before they were surplused. No

one was accountable for sanitizing the equipment before it was resold.

As a result of this incident, obsolete computer equipment (which includes monitors, mice, keyboards, etc.) is no longer resold, but destroyed. The Department of Energy learned a difficult lesson and now takes drastic measures to assure that no information is compromised.

University Surplus

The University I work at auctions used computers to the general public. I curious if computer hard drives were completely erased before being sold. I emailed a friend who had purchased surplus computer equipment in the past and he verified that the computers he bought from surplus still had all information intact. He told me that a computer he had purchased from surplus still had information on it.

This could be a serious problem because personal files could have been stored on the computer. Since it seems a secretary used the computer there could be confidential personal files on it. The University also has a medical center so computers surplused from the hospital could contain confidential patient data.

I used to work in a department at the hospital and we made sure that every computer surplused was formatted and then a large magnet was used to make sure that the information was scrambled. This was our department policy, but I do not know if other departments had the same policy.

Was it up to the department surplusing the equipment or the individual computer user to make sure no confidential information remained on the drive? In areas where it is critical that information be kept confidential there should be a system of checks and balances in place.

Dotcom

Another breach of confidentiality occurs when a bankrupt company's computer equipment is sold to liquidators. These liquidators then resell the computers to other companies or individuals. Even though the company may be defunct, computer hard drives could contain trade secrets, financial information, and personal information. One former dotcom

employee decided she was going to be responsible for deleting all the files on her computer. She had a computer consultant help her and make sure that her personal files were actually deleted from the computer she was using.

Even if one person makes sure their personal information is removed from the computer, other computers could contain personal records which could be damaging. When dotcoms go out of business they should have a policy for deleting information from their magnetic media.

Non-profit

I talked to a representative from a non-profit company that told me they receive donated computers. He said it is their policy to tell donors to make sure all personal information is removed from the computer, but people still leave personal information. I was told they had received machines with personal financial records, a complete copy of a college professor's book, love letters, personal diary entries and so on. The non-profit wipes all hard drives before giving the equipment to schools. If the non-profit were malicious they could use the personal information found on the hard drives unscrupulously.

Problem

The crime of identity theft can be committed with only a few essential pieces of information. Such as a social security number and birthdate. There are between 500,000 and 700,000 cases of identity theft each year (NASA) and the number will continue to rise unless people protect their personal information. It’s too easy for a dishonest person to buy computers at a surplus auction and collect usernames, passwords, and various personal information. Victims of identity theft may spend years to restore their credit rating. Even if one is cautious when recycling personal computers their employer may not be as careful.

Higher cost does not guarantee proper sanitization of hard drives. The best method is to use a wiping program endorsed by the Department of Defense. If a company does not have the time or money to spend on software hard drives can be shipped to companies that specialize in sanitizing computer hardware.

Solutions (from least effective to effective)

- Delete personal files and empty the recycle bin -- This is the easiest way to remove personal files, but anyone with an undelete utility may be able to recover the deleted files. Passwords from the Windows registry may be recoverable. Information can be found about the websites that were frequented and information can be gathered from Windows temporary files.
- Use software programs such as SecureClean -- SecureClean allows removal of sensitive data without formatting the hard drive. It will permanently remove deleted email, securely remove files, and remove passwords written to the swap file.
- Use WipeDrive, Norton Utilities Wipe, gdisk, or other secure wipe software – These utilities completely erase the hard drive regardless of the type of partition. The programs can be used to overwrite data on the disk multiple times.
- Use a high-energy magnet to erase the drive – This method should be used in conjunction with a utility such as WipeDrive. Magnets should be used with care around media that is not to be destroyed.
- Destroy the hard drive by taking a hammer to it – Again, this method works well in conjunction with the other methods.

Alternative solutions which could be combined with those listed above

- Use a hard drive password – If a computer has the ability to set a hard drive password it should be used. A problem arises if the user forgets the password and looses access to data. However, confidential information can still be retrieved by knowledgeable persons even if the hard drive has a password.
- Use strong disk-based encryption – This only works well if the whole hard disk is encrypted.

Policy

If there is no company policy on disposal of recycled computers, then one should be written. The first thing to be determined is the sensitivity of the information on the hard drive. If the only files on a hard drive are software

then formatting is probably sufficient. If the computer has been used for financial, medical, or tax purposes extra measures should be taken to be sure that data cannot be recovered.

The law varies from state to state, but in the state of Wisconsin, computer owners can be held accountable for any confidential information left on a hard drive or other magnetic media. Violators could face both civil and criminal penalties. This means a maximum fine of a thousand dollars or up to ninety days in prison (Wisconsin Manufacturers & Commerce). Since hard drives are so inexpensive it might be preferable to format the drive, use drive wiping software several times, then use a high powered magnetic to scramble the data before destroying the hard drive. It can then be insured the data will be extremely hard if not impossible to recover.

Once a policy has been developed that fits an organization's goals and values it is then necessary to secure the support of management. Managers must understand that it is not effective to only delete files from a computer's hard drive before sending the computer to surplus. Software wiping programs must be run several times to ensure that it will be unlikely for data to be recovered. If time or resources are not available to make sure the data are securely deleted or if management does not feel comfortable with the wiping software that is used, vendors are available to purge information from drives for a fee.

Conclusion

In today's throw away society old computers are a dime a dozen. Instead of throwing old computers away they can be given to non-profits, schools, or even auctioned off as surplus. Before a computer is thrown away, one should make sure there is no confidential information remaining. Businesses and individuals, should have a policy of removing all confidential information before a hard drive is discarded. Once a policy has been made it must be enforced and periodically checked to make sure confidential information is sanitized properly. The time and money spent on a good drive-wiping program is worthwhile. Think twice before pitching that old hard drive or computer because it could have information on it that someone might find very interesting.

References

Bucci, Pete. "Data security gets easier for surplus." The Business Review. April 3, 2000. URL: http://albany.bcentral.com/albany/stories/2000/04/03/focus6.html

Costello, Timothy G., and Anderson, Erik C.. "Dumpster Diving Law effective Feb. 1, 2000". Wisconsin Manufacturers & Commerce. URL: http://www.wmc.org/gr/hr/dumpsterdiving.htm

Garfinkel, Simson. "The Net Effect: Remembrance of Things Past." Technology Review. April 2001. URL: http://www.techreview.com/magazine/apr01/garfinkel.asp

Lee, Mie-Yun. "Don't Just Delete Computer Files, Shred Them". Business Week Online. November 16, 1998. URL: http://www.buyerzone.com/software/business_software/shred.html

Nelson, Ann Massie. "Does the New Dumpster Diving Law Apply to You?". Wisconsin Lawyer. March 2000. URL: http://www.wisbar.org/wislawmag/2000/03/risk.html

Orr, Tony Lee. "Oops—Energy facility fails to wipe data from surplus IT". Government Computer News. July 3, 2000. URL: http://www.gcn.com/vol19_no18/news/2347-1.html

Pippenger, Wesley E. "Protect Yourself and NASA Before Getting Rid of That Old Home Computer". NASA. March 22, 2001. URL: http://www.hq.nasa.gov/office/oig/hq/identity.html

Toler, Samuel. "Do You Know What's Left on your Disk?". October 20, 2000. SANS. URL: http://www.sans.org/infosecFAQ/covertchannels/remanence.htm

WhiteCanyon Software Inc. "How to Wipe Your Drives". URL: http://www.whitecanyon.com/library_how_to_wipe_disk.htm