The Corporate Risks Associated with Obsolete Computer Equipment

Daniel G. James

Abstract

This paper will discuss the risks posed by obsolete computer equipment in a corporate environment. Many people may not ever think about these risks as their new computer or laptop is installed and their old outdated machine is hauled off. However, those who are security minded will immediately inquire what is to be done with the old drive that is still full of data? The answer to this question varies by organization. Surprisingly there are companies who simply do nothing more that palletize old equipment and auction it off! Other companies have a more reserved approach and take the time to format the hard drives before donating them to charity, needy families, employees, or a local public school system. Each of these scenarios has large data security risks that have not been considered before action was taken. The data on these devices could cost the company millions or perhaps billions of dollars based on the type of data present. Each data storage device has its own level of risk. Data storage devices can include servers, desktop and laptop computers, printers, copiers, scanners, CD\RW, DVD\RW, floppy disk, USB thumb drives, DLT tapes, and the list goes on. This paper will reveal some of these risks and offer some possible solutions. Although risks are common among all corporations the solutions will vary based on application. This paper is intended to raise the awareness of these risks and get you started on the road to minimizing these risks to an acceptable level or eliminating them all together.

Surplus Computer Equipment is a Growing Concern

Ever wonder what happens to the old computer equipment at your company? Chances are there may be some managers or executives wondering the same thing! There are many companies, large and small, that never consider the risks associated with purchasing computer equipment and how to get rid of it at the end of its lifecycle. If a company has 10,000 pieces of computer equipment in production with a three year lifecycle turnover, there will constantly be a supply of surplus computing equipment. A company this size can expect to have around 3,000 pieces of surplus computer equipment every year! This equipment can be a mixture of desktop computers, laptops, scanners, printers, monitors, thin clients, servers, external hard drives, etc. Many companies are overwhelmed at the thought of processing this equipment and opt to simply get rid of it as quickly as possible deeming it unusable by their standards. The unfortunate thing about this scenario is that in most cases the equipment is still usable and full of corporate data! This data can include company secrets, social security numbers of personnel, patient data, credit card numbers, or whatever type of information is related to the business of that particular company. This data has now been compromised and could possibly fall into the wrong hands and be used against the company. On the other side of the scenario, this data could be discovered and published by the media giving the company bad press and a public sense of negligence. Who would want to do business with a company that is so careless with your personal data? This type of exposure could cripple or perhaps bankrupt a company.

Beyond the data security risks there are also environmental risks associated with surplus computer equipment. All electronic equipment contains non biodegradable materials that need to be disposed of or recycled in a certain manner. Cathode Ray Tube style computer monitors contain lead, phosphorous, and other dangerous materials that cannot and should not be placed in a landfill. If this is done the water table can be contaminated and adds to the already growing global pollution problem. This risk can also hurt your company with negative publicity and also financially if fined by the Environmental Protection Association (EPA).

Examining the Risk of Residual Data

"So, how can data be protected? How about selecting all of the sensitive files and pressing the delete key? How about formatting the hard drive? The truth is that many people see these methods as a secure way to destroy their valuable data, but they are wrong! It is very easy for even a novice user to recover some deleted files with freeware products available for download on the Internet. Formatting and using the recovery disks are effective deterrents for casual data snoops, but a determined hacker can dig into the guts of the hard drive and carve out old data. The magnetic surface of the hard drive has residual traces of the data, which, with perseverance and the right tools, can be recovered." (James, 2006) Consider this real life incident, "Utah State Auditor Auston Johnson conducted a "sting" operation a year ago that found important information — including Social Security and credit card numbers — on a handful of state surplus computers that were heading toward public sale. Credit card numbers, e-mails, private pictures, motor vehicle safety inspections, Human Services child and family case

information, criminal court histories, and even individual medical data were found on the surplus hard drives, Johnson said. In some cases, the hard drives had not been "scrubbed" at all. One computer was reported as "dead," meaning it could not boot up, so department officials just sent it off to Surplus Property. But Johnson's auditors took the hard drive out, put it in another computer and it started up fine, with all the information on it. In most instances some attempt had been made to scrub the hard drive, but it was somehow botched, and some information was retrieved "by simply buying recovery software off the shelf at any computer store and running it," said Johnson." (Bernick, 2007) This type of publicity for a company would do considerable damage to its reputation.

Consider again this real life scenario, "Fulcrum Inquiry analyzed 70 used hard drives purchased from 14 different sources. Most of the drives purchased were supposedly cleansed of all information. Peskaitis and Schultz also asked for the process that was used to clean the drives, and were usually told that the drives had been low-level formatted. Using computer forensics, Fulcrum Inquiry attempted to recover information from these hard drives. Admittedly, the tools used by the duo are complex and technical, but electronic-knowledgeable thieves can - easily - do what they did. From the disks that actually worked, Fulcrum Inquiry recovered private data from almost two-thirds (62 percent) of the disks. Specifically:

- 37 drives (53 percent) contained recoverable information
- 23 drives (33 percent) had been properly wiped/cleaned
- 10 drives (14 percent) were non-operational

The properly cleaned drives were either (i) low-level formatted or (ii) wiped using special software that overwrites data." (Peskaitis, 2007) Based on these two real world examples alone, it is easy to see that there is a huge risk associated with surplus or obsolete computing equipment. It is easy to wonder how many incidents have taken place that have yet to be discovered! The question now is how do you reduce or eliminate this risk? There really is not an easy answer that fits every situation. However, a good baseline security procedure would be to sanitize every data storage device after use with a DoD certified disk wiping tool or destroy them (James, 2006). According to NIST, "Advancing technology has created a situation that has altered previously held best practices regarding magnetic disk type storage media. Basically the change in track density and the related changes in the storage medium have created a situation where the acts of clearing and purging the media have converged. That is, for ATA disk drives manufactured after 2001 (over 15 GB) clearing by overwriting the media once is adequate to protect the media from both keyboard and laboratory attack." (Li, Kissell, Scholl, Skolochenko, 2003) There also must be an audit control in place to verify that the data has been securely deleted. Bulk degaussing, drive shredders, or pulverizing machines should be used for all data storage devices that cannot be securely wiped clean such as CD\RW, DVD\RW, floppy disks, DLT, optical, or hard disk drives that will not spin up due to malfunction.

There have been occasions where malfunctioning disk drives are returned under warranty to the manufacturer only to be refurbished and redeployed with your sensitive data still on them. (Sullivan, 2006) It is advisable to wipe these disks before returning

them. If this is not possible, enter into a contract with the hardware supplier before purchasing the equipment with the mutual understanding that any data storage devices will not be returned for any reason unless it has been securely wiped of all data.

Perhaps the hardest surplus data storage device to track and control is not surprisingly the smallest and most compact, the USB flash drive. "Any USB Flash device introduced to a network environment poses a grave risk to an organization's overall security posture. In most organizations, these micro drives bypass all established security mechanisms such as firewalls, intrusion detection systems and antivirus applications. Identifying these devices prior to use is nearly impossible, since most are miniaturized. These devices can be camouflaged to resemble a car key fob or an LCD flashlight. They can even be hidden in common objects, like the bottom of a coffee cup or large belt buckle." (Bumgardner, 2003) These devices can be wiped and or destroyed if you are able to keep track of them within your organization. This is why asset control and tracking is so important. A ten dollar USB thumb drive may not seem like an asset, but it can potentially hold gigabits of sensitive information worth millions to your company! Sure, there will be some folks in your organization who purchase these devices themselves and bring them into work, but this can be elevated somewhat with a good security awareness program or corporate security policy. In any case the use of any non-company owned data storage device should be strictly prohibited without proper training, and some type of encryption on the device if it is portable.

"Another device that is lesser known for its security risk but is a potentially huge threat is the photocopier. Many people use these devices everyday without the knowledge that there is a hard drive inside just like a computer! If your model is equipped with a hard drive, every document you scan, print, fax, or email through the machine is stored on its internal hard drive. Just think of all the tax documents you have copied, scanned, or emailed through your photocopier, and there is a good chance they are still there on that hard drive unencrypted in plaintext! I've not heard of any cases of ID theft from photocopiers. However, there is certainly ID theft in public places like Internet cafes and from kiosks, so I don't see why it couldn't happen at someplace like a Kinko's. Sharp was one of the first photocopier makers to offer a security kit that encrypts data on the hard drive and "shreds" each copied document by overwriting the image after it's printed. Rival Xerox Corp. introduced similar features on its machines last year. An organization should change the password from the default on copiers and multifunction printers. They should also disable all services that they do not need, and make sure that the data modem is separate from the fax modem." (Keiszer, 2007)

There are many different regulations that speak of obsolete computer equipment and what should be done with it. For instance, HIPAA's final security rule states "each covered entity must implement policies and procedures to address the final disposition of patient information (such as destruction of recycled disk devices)". (Smith, 2003) According to this rule, an organization that handles patient related data must have by law a secure way to dispose of this data! The bottom line is that there is an extreme data risk

associated with old computer equipment, and your organization should have a policy in place to address this issue.

Examining the Environmental Risk

Obsolete computer equipment does not only pose a data security risk or threat but also an environmental threat. "Computer equipment is a complicated assembly of more than 1,000 materials, many of which are highly toxic, such as chlorinated and brominated substances, toxic gases, toxic metals, biologically active materials, acids, plastics and plastic additives. The average computer has a lifespan of less than two years, and hardware and software companies are constantly generating new programs that fuel the demand for more speed, memory and power. Y2K concerns generated an increase in the number of new systems bought. According to the National Safety Council, as recently as 1994, buyers held on to their computers from four to six years. The San Francisco Toxic Coalition website states that three quarters of all computers ever bought in the US are sitting in people's attics and basements because they don't know what to do with them. At the end of last year another 24 million computers in the United States had become "obsolete". Only about 14 percent (or 3.3 million) of these will be recycled or donated. The rest - more than 20 million computers in the U.S. -- will be dumped, incinerated, shipped as waste exports or put into temporary storage in attics, basements, etc. In contrast, for major appliances such as washing machines, air conditioners, refrigerators, dryers, dishwashers and freezers, the proportion recycled in 1998 was about 70 percent of the number put on the market that year." (Wood, 2003) "There are significant regulations in place at local, state, and federal levels for proper computer disposal of the 6-8 pounds

of hazardous waste in a common PC. Following those regulations is not the major vulnerability. The real, but unseen danger for an organization is the fact that the original owner (or user if leased) is liable for disposal and that liability not transfer when the equipment changes ownership! If an organization passes their equipment to another party for use (employee sale, charitable donation, or sold in the market) an improper computer disposal down the line can come back to the original registered user." (Seybold, 2006) "With the recent increase in businesses offering computer disposal service organizations still have a need to ensure the proper handling of their disposed equipment. There are companies that disassemble or de-manufacture computers in to recyclable raw materials. Others export the equipment for resale, and some employ dumping in landfills. Since the original owner may be found liable, organizations need to research any recipient of their equipment to find out how they will dispose of it in the future." (Seybold, 2006) Here is a list of different toxins found in common desktop computers:

- Lead – "Found in cathode-ray tubes, solders. Each cathode-ray tube can contain five pounds of lead or more. Can cause damage to the central and peripheral nervous systems, blood system and kidneys in humans. Damage to a child's brain development has also been noted." (SVTC, 2007)
- Cadmium – "Printed circuit boards, semiconductors. By 2005, a total of more than 2 million pounds will exist in discarded computers. Cadmium and cadmium compounds accumulate in the human body, in particular in kidneys it is adsorbed through respiration but is also taken up with food. Cadmium can easily be accumulated in amounts that cause symptoms of poisoning." (SVTC, 2007)
- Mercury – "Batteries, switches. By 2005, 400,000 pounds across the US.

Methylated mercury causes chronic damage to the brain." (SVTC, 2007)

- Chromium – "Used as corrosion protection in steel. By 2005, estimated 1.2 million pounds. Chromium VI can easily pass through membranes of cells and is easily absorbed producing various toxic effects within the cells. It causes strong allergic reactions even in small concentrations. Asthmatic bronchitis is another allergic reaction linked to chromium VI. Chromium VI may also cause DNA damage." (SVTC, 2007)
- PVC Plastics – "Cables and housings. Potential waste of 250 million pounds per year. An MCC study estimated that the largest volume of plastics used in electronics manufacturing (at 26%) was polyvinyl chloride (PVC), which creates more environmental and health hazards than most other type of plastic." (SVTC, 2007)
- Brominated Flame Retardants – "Used in electronic products as a means for reducing flammability. In computers, they are used mainly in four applications: in printed circuit boards, in components such as connectors, in plastic covers and in cables. Scientific observations indicate that Polybrominated Diphenylethers (PBDE) might act as endocrine disrupters. Research has revealed that levels of PBDEs in human breast milk are doubling every five years and this has prompted concern because of the effect of these chemicals in young animals." (SVTC, 2007)

Conclusion

Many people do not realize the risks associated with incorporating IT in their organization. The risk goes beyond the production environment and follows the equipment to the grave. It is up to each organization to identify their risks and to mitigate each of them accordingly. The two risks covered in this paper are a good place to start and should be written into policy. The policy should include an asset tracking system, details on how the data storage devices should be sanitized or destroyed, a method of recycling per EPA, local, and state guidelines, and lastly an audit process to ensure each process is being carried out in a sufficient manner. If the audit control is absent there is a higher risk for errors in each process. "A great deal of expense is always encountered after the compromise, and it is always substantially more than the security plan and personnel needed to implement a security plan. This is not a new science – ask any accountant, and he or she will tell you, opportunity cost is 1000%." (Stoneman, 2003) There are many companies that find it is cheaper to outsource this burden than to hire in house staff to oversee the process. There are many reputable companies that will pickup your equipment, cleanse your data storage devices, recycle per all applicable guidelines, provide a certificate of destruction of each device, and audit the whole process for you for a fee. Before getting involved with any company, it is advisable to perform an onsite audit of their facilities before signing a contract. You must always weigh the risk of trusting your data to someone else, as opposed to developing an in house final disposition process.

Works Cited

Bernick Jr, B. (2007, January). Deseret News. *Data Found on Surplus Computers* Retrieved July 5, 2007, from the World Wide Web: http://www.deseretnews.com/dn/view/0,1249,660220231,00.html

Bumgarner, J. (2003, December). ISSA Journal. *Are USB Flash Drives a Security Threat to the Enterprise?* Retrieved July 5, 2007 from the World Wide Web: http://www.issa.org/Members/Journal.html

James, D. (2006, November). InfoSec Writers. *Forensically Unrecoverable Hard Drive Data Destruction*. Retrieved July 5, 2007 from the World Wide Web: http://infosecwriters.com/texts.php?op=display&id=525

Keiszer, G. (2007, March) Computer World. *Photocopiers: The Newest ID Theft Threat*. Retrieved July 5, 2007 from the World Wide Web: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9013104&source=NLT_WK&nlid=2

Li, X. Kissel, R. Scholl, M. Skolochenko, S. (2003). National Institute of Standards and Technology. *Guidelines for Media Sanitization.* Retrieved July 5, 2007 from the World Wide Web: http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

Peskaitis, S. (2007, February). eWorldWire. *Computer Forensic Study By Fulcrum Inquiry Reveals Computer Hardware Sellers Are Selling More Than Expected.* Retrieved July 5, 2007 from the World Wide Web: http://www.eworldwire.com/pressreleases/16402

Seybold, R. (2006, December). TechDisposal. *Common Mistakes in Disposal or Retirement of Computer Equipment.* Retrieved July 5, 2007 from the World Wide Web: http://www.techdisposal.com/Land.aspx

SVTC. (2007, July). Silicon Valley Toxics Coalition. *Toxics In Electronics: 1000's Of Chemicals are Used In Electronics Products.* Retrieved July 5, 2007 from the World Wide Web: http://svtc.etoxics.org/site/PageServer?pagename=svtc_toxics_in_electronics

Smith, H. E. (2003, October). ISSA Journal. *The HIPAA Final Security Rule – More Than a New Security Standard*. Retrieved July 5, 2007 from the World Wide Web: http://www.issa.org/Members/Journal.html

Stoneman, D. (2003, May). ISSA Journal. *Lessons Most Companies Have Not Learned*. Retrieved July5, 2007 from the World Wide Web: http://www.issa.org/Members/Journal.html

Sullivan, B. (2006, June). MSNBC. *Red Tape Chronicles: I Just Bought Your Hard Drive.* Retrieved July 5th, 2007 from the World Wide Web: http://redtape.msnbc.com/2006/06/one_year_ago_ha.html

Wood, L. (2003, June). Galt Global Review. *Old PC's Toxic In Landfill Sites*. Retrieved July 5, 2007 from the World Wide Web: http://www.galtglobalreview.com/business/toxic_pcs.html