Closing the Back Door: Managing IT Data Security During Equipment Disposal

By: Kevin Myrant and Neil Peters-Michaud
April 28, 2005

Executive Summary

Companies invest significantly in securing data in their information technology (IT) equipment during procurement, implementation and use. Many times, regulation requires them to maintain certain controls and a chain of custody for personal information captured on IT equipment. Yet, with all of this investment and time dedicated to installing firewalls, password protection, and physical guards to prevent data theft, companies may neglect to manage the data on older IT equipment once the assets are retired from use. This paper provides information on how to extend best management practices for data security to IT assets designated for retirement, and it dispels some myths related to various data destruction options.

Keywords:

Data Security, IT asset retirement, HIPAA, FACTA, Wipe, DoD 5220.22-M

Threats to Data Security

Privacy protection and identity theft have gone from being a rare and sensational media curiosity to an agonizing fact of life impacting 1 in 6 adults in the United States in the past decade, according to the Justice Department[1]. Numerous examples of compromised business and institutional security systems make headlines in the press. Often, these tragedies illustrate how active network systems can be hacked or individuals can be spoofed to release private information.

Similar examples of breaches in an organization's data security system can be found once systems come off line and are thought to have been safely disposed. The following news reports present some specific incidents of data leaks from IT assets retired or removed from a corporate environment.

- "Over two years, Simson Garfinkel and Abhi Shelat bought 158 used hard drives at secondhand computer stores and on eBay. Of the 129 drives that functioned, 69 still had recoverable files on them and 49 contained 'significant personal information' -- medical correspondence, love letters, pornography and 5,000 credit card numbers. One even had a year's worth of transactions with account numbers from a cash machine in Illinois." [2]

- "The disappearance of a laptop hard drive in the California State University (CSU) system has triggered a year-old state law requiring anyone whose personal information

© Cascade Asset Management, LLC, 2005. All Rights Reserved. The information contained herein has been obtained from sources believed to be reliable. Cascade disclaims all warranties as to the accuracy, completeness or adequacy of such information. Cascade shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof.

might have been stolen to be notified. The hard drive, which contained names, addresses and Social Security numbers for some 23,000 students, faculty members and employees at seven CSU campuses, is believed to have been accidentally thrown away after it was replaced by an IT technician, said Clara Potes-Fellow, a spokeswoman for the university's chancellor's office. 'We have not had any cases of identity theft' related to the incident, she said. But under the new law, letters were mailed to all 23,000 people affected by the data loss in late July to inform them of the situation."[3]

- "Christus St. Joseph Hospital sent a computer to Gateway file systems to transfer hospital records onto a digital format. But burglars broke in and stole the computer before that could happen. On the hard drive were names, Social Security numbers, and medical information, which was protected with a password, but experts say that's no guarantee. "There is always vulnerability when it comes to passwords. No computer password is safe," said computer expert Michael Garfield."[4]

- "This week's 'Spiegel' - one of Germany's leading weekly papers has revealed that a computer hard drive with confidential data from the Brandenburg police in Germany has been auctioned over eBay for a mere 20 Euros. The used hard drive with 20GB capacity contained, according to Spiegel, internal alarm plans on how the Police should handle 'specific incidences' such as hostage or kidnapping situations, gave contact names of who to contact in the crisis management group as well as tactical orders and analysis of political security situations. Such information is declared strictly confidential and is available only to top level people of the intelligent services, the head of police, and the executive group around the Minister of Interior Schönbohm."[5]

These examples illustrate the fact that enterprises are vulnerable to data theft even after their IT assets are disposed. Many companies fail to recognize the prevalence of their data storage devices – from hard drives to back up tapes to cell phones and PDA's with contacts and calendars to paper with references to passwords and access codes. Any media that records data provides an opportunity for identity theft until it is destroyed.

Responding to Security Threats with Investments during Procurement and Use

A large body of software, hardware and service professionals has emerged to prevent and respond to security threats in enterprises. The cost to protect IT assets is comprised of investments in hardware and software for individual workstations and networks, as well as personnel expenses required to install and maintain these systems. Computer Economics determined the annual cost to provide a secure environment for a medium risk business with 500 nodes to be $116,626. At the same time, their report claims the economic impact of malicious attacks on this type of business to run at $203,600, therefore justifying the investment in security systems.[6]

© Cascade Asset Management, LLC, 2005. All Rights Reserved. The information contained herein has been obtained from sources believed to be reliable. Cascade disclaims all warranties as to the accuracy, completeness or adequacy of such information. Cascade shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof.

Table 1: Annual costs and ROI for Security in a Medium Intensity E-Business Environment (prior to asset disposal)[6]

Number of nodes in the organization	Projected costs for computer security products	Projected costs for network security products	Associated personnel costs	Total projected security costs	Economic impact of malicious attacks	ROI for security spending (prior to disposal)
25	$2,500	$987	$2,256	$5,743	$12,025	$6,282
50	$5,200	$1,974	$4,418	$11,592	$25,200	$13,608
100	$9,900	$4,160	$8,742	$22,802	$46,674	$23,873
250	$23,300	$11,045	$21,902	$56,247	$108,375	$52,128
500	$45,900	$22,490	$48,236	$116,626	$203,600	$86,975
1,000	$81,200	$75,200	$97,297	$253,697	$402,225	$148,528
2,000	$148,500	$106,455	$195,826	$450,781	$787,350	$336,569
3,000	$207,800	$166,709	$297,416	$671,925	$1,244,970	$573,045
5,000	$324,800	$287,969	$500,973	$1,113,742	$2,243,875	$1,130,133
10,000	$617,200	$591,166	$999.925	$2,208,291	$4,065,416	$1,857,125
20,000	$1,100,000	$763,750	$1,750,750	$3,614,500	$7,231,488	$3,616,988
50,000	$2,784,000	$3,097,300	$5,070,360	$10,951,660	$16,789,500	$5,837,840

IS departments spend a great deal of time and energy in managing their existing security systems, by regularly updating filters, forcing users to switch passwords, and securing back-up systems. Privacy protection requirements from FACTA, HIPAA, GLBA, and numerous state regulations force companies to account for all data collected, stored, and distributed. Unfortunately, these well designed systems are only as strong as their weakest link.

Recognizing "Back Door" Security Threats

What happens to the obsolete equipment the day after the big rollout when much of the focus is on managing new equipment? In too many cases this equipment is stored in public access hallways, garages, or unlocked basements until decision makers can schedule its disposal, leaving critical information available for employees, visitors and customers to view, copy or steal. Some firms still toss their IT equipment in the garbage where it can easily be hauled off by social engineers or dumpster divers. Simple data retrieval programs can often hack into information left unprotected by firewalls and network protocols. Sometimes, users make a theft easy when they mark their passwords on the equipment making the process more accessible to malicious activity.

In order for an enterprise of any kind to have a truly secure information system it must have a method of disposal for retired equipment that prevents data from being recovered once it leaves its securely managed environment. This safely closes the circle that is the life cycle for an IT asset as well as responsibly manages the chain of custody for information held by an enterprise. To overlook this critical phase of the system life cycle is to waste all of the investments to purchase and implement the security of your present system. Expensive consultants, sophisticated software and powerful hardware will have done you no good if data is retrieved from even one data storage device and used against you maliciously.

Maintaining Physical Custody of Retired Assets and Archived Data

Physical access during the beginning phases of equipment is intuitive and controlled by placing the asset in a secure environment, populated work area or by virtue of its electronic status or continuous use. No one can steal a router, or server that is in constant operation and is monitored by access logs without raising some kind of alert.

Any time equipment is replaced, attention needs to be paid to archiving and securing the data on the old system. This may take place through a network backup, external tape, disc or drive back up, or physical removal of the hard drive. The archive should be cataloged, stored and secured

© Cascade Asset Management, LLC, 2005. All Rights Reserved. The information contained herein has been obtained from sources believed to be reliable. Cascade disclaims all warranties as to the accuracy, completeness or adequacy of such information. Cascade shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof.

for later retrieval. In addition, a backup inventory and archive schedule is an essential part of a security system to ensure backups are accounted for and stored only as long as is absolutely necessary. Once any reasonable need to store the archived data has passed, a method for secure destruction and disposal is in order.

Once the data on retired units have been archived, it is important to quickly neutralize or destroy the data on that equipment. Simple encryption programs can be run from the desktop on the unit prior to the final disconnection of the computer from an enterprise network. These programs lock access to a computer by scrambling the data.

More costly and time-consuming data wiping programs can also be run on hard drives. A typical one-pass overwrite of a 20-GB IDE hard drive takes about nine minutes. More secure 3 to 7 pass Department of Defense confidential data destruction compliant wipes take proportionally longer.

Finally, some companies open computer, laptop and server cases to physically destroy hard drives with drill presses or sledge hammers, among other tools. While effective at immobilizing the device, data can still be retrieved through forensic recovery, and the time and attention and potential safety risk involved in performing this task is typically not appropriate for an IS technician.

The more typical method for securing old data is through physical controls. Just as document destruction companies set up collection bins in offices with slotted and locked lids, electronic media destruction firms can offer those same totes for the collection of pulled drives, tapes, and other media for later destruction. If hard drives are kept in the existing system, the collection of older computers for off-site data destruction and media destruction could be coordinated to coincide with the deployment of the new systems. In this scenario, a secure media management firm takes custody of the equipment just as it is removed from the enterprise security system. The next best option is to package and store the equipment in a locked and secure room.

Here's where an asset management system provides value. If your company tags and tracks IT assets throughout their lifecycle at the enterprise, a simple scanning or notation of retired assets in the system and indication of their status will provide a wealth of information when looking for redeployment or retirement options. It will also provide documentation of the assets removed from your on-site security system and transferred to another responsible party. Asset management is now a required feature of maintaining a responsible chain of custody for electronic media. This information can be shared with off-site IT retirement firms who can provide reasonable costs or values for this equipment and who can demonstrate that the information on each asset was destroyed properly. Tracking and cataloging assets can greatly reduce handling and disposition costs later.

Off-Site Destruction of Information

Although there are low cost and even no cost methods of disposing of your IT equipment, they often come with a great deal of risk and expose you to liability which far exceeds the short term financial benefit. The primary goal of responsible care in destruction of information is to do it as soon as possible. The further data travels through the disposition process, the greater the risk. From the truck driver willing to pilfer his load of laptops on the way to the disposal company, to the overseas computer refurbisher using the licensed software on a PC "recycled" from the US, to the social engineer actively hunting for information to exploit, there are numerous threats to information throughout the disposal process. The effects of using inferior and risky disposition methods are essentially cumulative.

© Cascade Asset Management, LLC, 2005. All Rights Reserved. The information contained herein has been obtained from sources believed to be reliable. Cascade disclaims all warranties as to the accuracy, completeness or adequacy of such information. Cascade shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof.

When contracting with off-site vendors for destruction services, inquire about the following practices:

- What information security management practices and technology do they employ? Their level of investment and attention to their own security needs is often indicative of their handling of other's information.
- What type of insurance or bonding does the vendor carry to cover data leaks?
- What asset management system does the vendor use to effectively track and report on the disposition of equipment?
- What technology does the company use to electronically wipe or physically destroy equipment? Where does this technology exist and what steps must the equipment go through before it is destroyed?
- Can destruction of personal assets be witnessed?
- What happens to the destroyed assets after the vendor completes its work?

Transferring title and responsibility of equipment to a third party also includes a transfer of risk. Certain regulations require third parties handling personal privacy information to commit to a Business Services Agreement that outlines the responsibilities and activities of the vendor when managing information transferred to them.

When many enterprises audit their IT asset retirement company or recycler they look to assess the vendor's environmental management system to determine potential liability exposure related to hazardous waste treatment and disposal activity. More and more enterprises are also including security audits of vendors to ensure compliance with privacy requirements and to demonstrate a comfort level with the way their security systems and asset management services intersect.

Selecting a third party processor of disposed IT assets cannot be viewed as a nuisance, but must be recognized as an important extension of the management of information technology security systems.

Assessing Various Electronic Data Destruction Methods

Your specific security needs should be evaluated in relation to your company's regulatory requirements, corporate governance standards, the overall level of risk you find acceptable and the resources you have available to affect a solution.

Data destruction services exist on a continuum from least effective to most. The most elaborate solution is not always the best for every situation.

It is important to remember that the people trying to gain access are criminals. As is the case with crime, even some protection is likely to be somewhat effective. A criminal will often prey upon the "easiest target" to maximize their gains.

Failing to comply with your fiduciary, environmental and social responsibilities is dangerous and not recommended. However you must arm yourself with knowledge and analyze the benefits of any solution to avoid being "over-sold". Carefully weigh the realistic threats against the benefits of various solutions and evaluate the cost and benefits of each.

- Malicious misuse is most likely perpetrated by someone with only limited skills doing so for personal gain, revenge or as a prank. Luckily it is easy to foil such a person either

© Cascade Asset Management, LLC, 2005. All Rights Reserved. The information contained herein has been obtained from sources believed to be reliable. Cascade disclaims all warranties as to the accuracy, completeness or adequacy of such information. Cascade shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof.

with physical destruction or by overwrite of the entire data surface. Assuming you overwrite the data you could possibly recover some of the cost of doing so by resale of marketable equipment.

- Less likely and of more concern is the case where there is someone with professional level technical skills with a willful intent to capture your data. These people are more difficult to foil, but physical destruction and overwrites are still effective against most of their threats. Data could only be recovered by exhaustive efforts with costly equipment.
- Military grade overwrites are the most frequently requested service level, but the time, effort and cost far outweighs any gain made by resale of even high grade marketable assets.

Many people are under the mistaken impression that deleting files (moving them to the recycle bin and even emptying it) or formatting a hard drive in windows will render their data "unrecoverable". These methods make data appear not to exist. When you search for it within the operating systems search facility or even when you install the hard drive in another computer, you can quite easily retrieve it in whole or in part. These data still exist until they are either overwritten or the hardware is physically destroyed. The data will not simply go away, fade or disappear until one of the above methods is applied to it correctly.

A wide variety of electronic and physical data destruction methods have been developed over the years. They range from simple low-level reformatting of drives to full scale multi-pass wipes. Many people refer to Department of Defense (DoD) Compliant confidential data destruction techniques. This refers to two standards developed by the DoD for achieving certain levels of data destruction. These standards are often referenced by many in the industry. Other Standards exist as well and they are listed in Table 2.

Table 2: Selection of Standards for Electronic Data Wiping

Standard Name	Description	Reference
DoD 5220.22-M	Department of Defense developed: requires 3 or 7 pass wipes based on a succession of random or pre-set character overwrites of all sectors of data	http://www.dss.mil/isec/nispom_0195.htm
Russian GOST P50739-95	5 pass overwrite	
German VSITR	7 pass overwrite	
Gutmann Method	35 passes, with 27 random-order passes using specific data combined with eight passes using random data.	http://www.cs.auckland.ac.nz/%7Epgut001/pubs/secure_del.html

A number of software programs have been developed to wipe the information from hard drives according to the protocols of these and other standards. These programs may also perform low-level data scrubs, including reformatting and re-partitioning a drive. All of these methods are at least better than “dragging a file into the Recycle Bin” on a Windows desktop. Depending on the need for security, available resources and time, different wiping methods may be more appropriate. Table 3 provides an overview of various data scrubbing methods, their levels of destruction, and required resources to implement the technology.

© Cascade Asset Management, LLC, 2005. All Rights Reserved. The information contained herein has been obtained from sources believed to be reliable. Cascade disclaims all warranties as to the accuracy, completeness or adequacy of such information. Cascade shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof.

Table 3: Data Destruction Methods and Related Recovery Opportunities

Data Destruction Method Used	Description of recovery possibilities	Complexity of recovery	Resources needed for recovery	Who could do this?	Resale Residual
Format of entire drive or deletion of files	Operating system is restored to a fully usable state with all data intact	Simple - if you can follow directions such as wizard supplied with recovery software	Commercial software; Freeware/GPL software	Any user	Yes
Format of entire drive and deletion of partition table and both copies of file allocation table	Operating system is restored to a fully usable state with most/all data in tact	Slightly less simple - you must understand some specific computer terminology, find information and enter commands (about 3) in proper sequence and syntax	Commercial software; Freeware/GPL software	Any user	Yes
Deletion of Master Boot Record. Deletion of partition table and File Allocation Table. Format drive.	Operating system can still be restored with time, effort and skill. All data is easily recovered in complete and usable state	More steps than above to recover partition table. Many software packages will do this all for you in one contiguous process	Commercial software packages	Any user	Yes
Commercial software (e.g., WipeDrive, Blanco) – one pass wipe	Almost no data fragments of data without context (a few characters)	Nearly impossible	Combination of software and hardware specifically designed for recovery of data	Skilled forensic examiner laboratory setting	Yes
Commercial software (e.g., WipeDrive, Blanco) – multipass wipe	Almost no data is recoverable by anyone without special training and expensive hardware	Nearly impossible	Combination of software and hardware specifically designed for recovery of data	Skilled forensic examiner laboratory setting	No, cost of overwrite outweighs the value of the asset
Commercial grade/military certified degasser	Almost no data is recoverable by anyone without special training and expensive hardware	Nearly impossible	Combination of software and hardware specifically designed for recovery of data	Skilled forensic examiner laboratory setting	Degaussing destroys ability to write to data storage device. Commodities can be harvested for recycling.
Shredder	Data may be intact if no other method is applied to overwrite or destroy it prior to physical destruction	Physical drive pieces must all be found, unit is recreated and surface is analyzed	Electrostatic calibration equipment capable of measuring polarity and strength of small magnetic field created by each bit of data	Skilled forensic examiner laboratory setting	Destruction prevents reuse for anything. Harvesting of commodities for recycling.

Security managers should test the effectiveness of data removal techniques by attempting to recover data from the wiped media. Several commercially available disk restoration programs are available. (See http://www.xstudio.ca/pcsupport/system/datarecovery.html for a free demonstration of several recovery programs.) You can also audit your third party vendor by asking them to wipe several sample drives and then have them return the drives to you so that you may attempt a recovery.

© Cascade Asset Management, LLC, 2005. All Rights Reserved. The information contained herein has been obtained from sources believed to be reliable. Cascade disclaims all warranties as to the accuracy, completeness or adequacy of such information. Cascade shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof.

Determining the Appropriate Level of Data Destruction

Table 3 demonstrates that for any type of destruction method listed, there is a possibility the data can be retrieved through some type of recovery process. Many companies selling data security software and services will focus on these vulnerabilities and use fear to motivate you to purchase their product. A sense of reasonability must be applied to these scare tactics so that you can manage a level of security risk with an investment in security processes and technology. The same considerations are made when determining security systems for IT equipment when in use – companies are always vulnerable to security breaches, but they can take steps to mitigate these exposure levels to a reasonable tolerance.

No one method exists to completely remove the possibility of recovery. The method or methods that you choose must fit your needs and your budget. Realistic assessment and understanding the risks you face is your best defense. You must look at data security as part of a bigger solution and it must be done in concert with other security mechanisms to provide your organization with the most cost effective and sustainable solution.

In general, for most businesses and organizations, the most practical approach to managing the risks associated with recovery suggests that one overwrite of electronic media will foil all but the most determined, skillful and best financed threats. Subsequent overwrites add cost, reduce any potential return but don't really reduce the risk in any appreciable way unless your threats include:

- the federal government;
- foreign governments;
- military organizations;
- justice organizations;
- intelligence organizations;
- quasi-military organizations; or,
- technically sophisticated competitors with virtually unlimited resources.

In short, one successfully completed overwrite of the entire data surface will reduce your risks to the above mentioned threats. Also bear in mind that the cost and effort is so exhaustive for each asset that threats even of this nature will likely find other means of obtaining information or attacking you, such as cohesion, theft or “social engineering.”

Conclusion

When developing an information security system for your IT equipment, don’t forget about managing IT equipment after it is removed from service in your company. These items often contain a wealth of information that is vulnerable through electronic recovery or physical theft. All of the investment in infrastructure security can be wasted if attention is not paid to maintaining a secure archiving and disposal system. For most situations, developing a secure chain of custody within the organization with a trusted IT asset manager will go a long way to ensuring information is less vulnerable to theft or misuse.

About the Authors

Kevin Myrant is Special Projects Manager for Cascade Asset Management, LLC, where he has worked since 2001. He is responsible for data security compliance programs at Cascade. Previously, Kevin served in the United States Army Signal Corps, where he held a Secret Level Security Clearance. He also worked as a Combat Signaler in a forward command center. He

© Cascade Asset Management, LLC, 2005. All Rights Reserved. The information contained herein has been obtained from sources believed to be reliable. Cascade disclaims all warranties as to the accuracy, completeness or adequacy of such information. Cascade shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof.

provided mobile secure (encrypted) single channel retransmission communications support for a division level combat unit in an independent small team based environment. Due to the mobile nature of the unit (RETRANS), Kevin received advanced training in routine destruction of secret level documents and the intentional destruction encryption equipment to prevent compromise of secret technology. Kevin received an Army Commendation Medal (ARCOM) for performance of the above duties. He also earned his Associates Degree in Applied Science – Computer Information Systems from Madison Area Technical College in 2002.

Neil Peters-Michaud is co-founder and CEO of Cascade Asset Management, LLC. He earned a Master's in Business Administration from the University of Wisconsin in 1999 and a Bachelor's of Science from the UW in 1993. He was appointed by the Governor to the Wisconsin Legislative Council on Recycling and is co-chair of the 2005 International Symposium on Electronics and the Environment. Neil has been involved in electronics recycling since 1994 and has authored numerous papers and presentations on environmental, health and safety impacts of electronics recycling. Neil grew up in Silicon Valley and immersed himself in the IT industry through positions with several prominent electronics manufacturers.

---

[1] "Stop thieves from stealing you," *Consumer Reports*, October, 2003.

[2] "Discarded computer hard drives prove a trove of personal info," *Associated Press*, http://sfgate.com/cgi-bin/article.cgi?f=/news/archive/2003/01/15/national1617EST0765.DTL, January 15, 2003.

[3] "Hard drive with 23,000 Social Security numbers disappears," *COMPUTERWORLD*, http://www.computerworld.com/securitytopics/security/story/0,10801,95690,00.html,

September 3, 2004.

[4] "Hard drives found in dumpster could have made lives miserable," *The Beam*, http://www.dcmilitary.com/airforce/beam/10_14/local_news/34220-1.html, April 8, 2005.

[5] "Top Secret German Police Hard Drive Sold Over Ebay For 20 Euros," *I-Neswire*, http://i-newswire.com/pr13647.html, April 5, 2005.

[6] "The Return on Investment for Network Security," Cisco Systems, 2002.

© Cascade Asset Management, LLC, 2005. All Rights Reserved. The information contained herein has been obtained from sources believed to be reliable. Cascade disclaims all warranties as to the accuracy, completeness or adequacy of such information. Cascade shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof.