Global Information Assurance Certification Paper

Gerard Geggis
GSEC 1.4b
Systems Retirement: Secure Data Retention and Disposal

Summary:

As computer systems age it becomes desirable to replace them with more modern equipment. As a result, we have an abundance of computer hardware that contains confidential information. In some cases, that information needs to be retained, and, in other cases, it needs to be disposed of properly. These systems have data residing on many different type of media, such as paper hard copy, hard disk drives, floppy diskettes, CD-ROM's, and magnetic tape. In some cases, it is a device such as a PC or PDA that gets replaced.

Policies need to be created to determine how this information is to be retained, how to properly dispose of the media used to house the data, and how to remove any confidential data that remains on them. It is critical that these policies are consistently adhered to in order to avoid legal vulnerability. While, there is often more than one option available to remove data from a media, in some circumstances a complete destruction of the physical media is the only sure way to eliminate all traces of information. Each organization needs to evaluate its risk based on the level of data sensitivity, and the sophistication of those likely to attempt access of that data.

I. Data Retention of Retired Systems:

Many organizations retain data for many years, even after the systems that were originally used to create it have long gone out of use. There are a number of methods used to keep this information available to organizations. Whichever means is used, it is essential that it follow the corporate policy on the retention of data.

One way to retain the data is to keep the system that was used to create it in tact, but as a single user device that can be used to recall old data. These devices are often turned off except when there is a need to retrieve the data. In some circumstances the devices reside in the department that used the system, such as payroll, or accounts receivable, Human Resources, etc., and they are placed in relatively insecure areas. The access security on these older systems is often weak, and although an organization may have strict access and control policies, these systems are frequently overlooked. The administrator account is often the only account that is still operational, and therefore access is total, with no restrictions to data in the application. In some circumstances, the person, or persons who are familiar with the program leave the company, and new hires are not familiar with the system, or even its existence. This can lead to improper disposal of the system by someone who does not understand the sensitivity of the information it contains. If such systems are to be kept for future reference, they should meet current security protocols, and be maintained by the appropriate personnel to assure precautions are taken to keep the data confidential.

In some situations, the information is simply backed up onto magnetic tape, or even optical disk to be restored back when needed. The trouble with this scenario is that the tape drives or optical drives that originally created the media are often obsolete and unavailable. If this method is used, it is critical that a documented procedure for the storage and retrieval of the media be in place, and that the proper hardware be maintained in order to facilitate timely access to the data.

Many companies make print outs of the pertinent information from the system before it is taken off-line. While, this is sometimes an acceptable way of dealing with older data, care should be taken to secure the documents so that there is limited access to them, and so that they are not disposed of prematurely. However, in some instances this method may not meet regulatory requirements.

Of course the most desirable way of dealing with this information is to convert it into the new software that is being used to deal with such data. It is common to bring it over as archived data. This allows use of the security infrastructure of the new system, which should be up-to-date and conforming to the organization's security policies.

Sometimes bringing data directly into a new program is not possible or feasible. In such cases, one could attempt to convert the data to a more standard format, such as ASCII text, or a spreadsheet. This could be difficult, depending on the amount of information that is necessary to keep (for example, large databases probably would not function well in this scenario). This would allow for controlled rights to the file, such as read-only or read-write, etc. The access would not be granular, however, meaning that anyone with rights to read the file would have access to all the data in it.

In whatever manner the data is to be maintained, it should be remembered that it should only be retained for as long as the data is truly viable. Data that is not needed should not be retained, as it usually creates security and legal risks. Many organizations have certain legal requirements that they must follow, and there are often many good reasons to keep data for several years, but these should be outlined in a corporate policy that states how long certain types of data are preserved for legal and/or business reasons.

II. Destruction of Data:

As the information that a system holds becomes obsolete it must be disposed of properly. This data can exist on many different media. The types of media that are used to hold data and the proper disposal methods that should be used are detailed below. Often, there is more than one way to dispose of data. It is necessary to do a risk analysis of your data to determine how far you need to go for each type of media.

A. Paper:

The printed word is one of the media that are very difficult for an information security person to control. Almost every user on a given network has access to some confidential information, and the ability to print it. Once it is printed, it is in the control of the user that handles it. Proper policies should be in

place that outline how users handle this data including what they do with it when it is no longer needed.

While there are many methods used for the destruction of paper products, the two most commonly used are shredding and burning. There are several ways to address how shredding or burning are to be done in a corporate setting.

1. Shredding:

The strip cut shredders are generally the least expensive devices used in medium or large-scale environments. This basic technique produces a bag of strips that would be difficult to put back together. While this method of shredding is preferable to simply ripping the paper by hand, crosscut shredders produce much smaller pieces by cutting the paper in both horizontal and vertical directions. The final result is such that the document is virtually impossible to recreate. Additionally, it produces a denser end product that takes up less space in dumpsters. The DoD has requirements on maximum size the pieces that are created can be (1/32 inch in width by 1/2 inch in length) for classified documents[1].

2. Incineration:

If an incinerator is available and practical, burning is a viable option for paper destruction, keeping in mind that the complete incineration should to be visually verified.

3. Contracted Destruction:

Both of the previous options are available to various sized organizations. They are good for areas that have a small to moderate amount of material that needs to be destroyed. For some business, a large volume external company could be used to perform these services. Many of these firms will now shred on-site; this is important, because if the documents (in their original, non-shredded state) are on a truck, and something happens (and it has) while it is in transport, confidential data can end up floating around on the highway for anyone to pick up and read.

4. Summary of Paper Destruction:

There must be a paper disposal policy that details the controls to assure proper handling of paper material as it moves through the system from the source of origination to those responsible for its destruction. All the people involved must realize the sensitive nature of the material that they are handling, and take appropriate precautions to safeguard its privacy. This is even more important when an outside vendor is used to dispose of sensitive documents. There should be contract language that states that suitable destruction is being confirmed. However destruction is done, equipment must be properly operated and maintained. Most importantly, in all cases, the destruction of the data must be verified.

[1] DoD, chapter 5, section 7.

B. Magnetic Media Disposal:

Magnetic media such as diskettes, hard drives, and tapes all use similar recording and erasing techniques.

1. Magnetic Media Erasure Techniques:

There are a few different methods that can be used to make the data on a magnetic media inaccessible. Each has its benefits and drawbacks. Each method can be used on the media discussed in this article, but some are less practical for certain types of media. For instance, while diskettes and hard drives are relatively easy to overwrite, it is not so simple to do so effectively on most tape media. Whereas, tapes and diskettes can be easily burned beyond recovery, it is a little more involved to prepare a hard drive for destruction through incineration.

a. Over-write Method:

This is probably the most common method of clearing data from a hard drive. Unfortunately, the original data can often still be retrieved with some widely available tools and services. Retrieval of original data can be made more difficult to accomplish by performing several over-writes to each sector of the media.

When an over-write is performed, the disk or tape drive is not capable of writing to the precise same location as where the original information was located so that traces of previously stored data still resides on the media. Although it is a very tedious process to get even the smallest of useful information, it is possible for an individual with little training to peel back one or two overwrites using a high-quality sampling digital oscilloscope. Using a technique called magnetic force microscopy, even several over-writes can be overcome. This can be done using a scanning tunneling microscope (STM)[2]. While these devices are not available to everyone, there are several resources on the web on how one can be built. One could also utilize a data recovery service that employs this technology to recover lost data.

These techniques can be thwarted by over-writing each track several times using alternating patterns during each over-write. Some over-write methods combine random writes with exact varying bit patterns to mask the different layers of information. One such example from Peter Gutmann's paper "Secure Deletion of Data from Magnetic and Solid State Memory" utilizes 35 separate overwrites; others actually recommend at least 105 overwrites[3].

The DoD outlines a basic overwrite process in document 5220.22-M, chapter 8, but the minimum standard is only three overwrites (one of specific pattern, its compliment, and then a random pattern), and does not meet the recommendations listed above. An example of the DoD recommendation is to write all ones, then all zeros, and a random pattern combination of ones and zero's. If this method is used, it is likely anyone wishing to access the information could do so using magnetic force microscopy.

---

[2] Gutmann, p. 2.
[3] Genio, p.3.

There are a number of disk over-write products available that utilize the strategies listed above. While overwriting data is relatively inexpensive (some of these programs are freeware), it does require many passes on the disk surface, and, therefore, is time consuming and patience is require of the operator to make sure that the data is thoroughly overwritten.

When dealing with disk drives it is common to have areas that have been marked as bad blocks that will not be over written by this process. If there was data stored in this area before it was marked as bad, it will not be overwritten. These areas should be taken into consideration if sanitation of the device is required.

b. Degaussing:

Degaussing is a method whereby the magnetic media is subjected to an alternating magnetic field that turns the media back to a neutral state. At this point, the media is seen as blank. In some cases, the media is rendered unusable, because the servo signals that manufacturers place on their media get deleted. In all situations, once properly degaussed, the media should be ready for disposal. This is the method that is most widely used for tape media; although, it also works well on diskettes, and most hard drives.

The term coercivity is used to describe the magnetic field strength necessary to destroy data on a given media. This is measured in oersteds (Oe). Degaussers are required have an Oe higher than the media being erased in order to effectively clear the data

Degaussers come in many different types, sizes, and strengths. Some are single purpose units that only erase tapes, some are tailored toward erasing hard drives, and some are all purpose units that will erase any media type that is rated below its own Oe value. Some degaussers are simple hand held devices that can be pretty powerful, but can only handle very low volume applications, while others are large devices that can handle several media at one time.

The method of degaussing can vary between degaussers. On some general-purpose degaussers, it is recommended that a media should have as many as four passes on the degausser; rotating it on each pass. For example a tape should degaussed topside down, and then rotated 90 degrees, degaussed on its side, the other side, and finally degaussed bottom side down; on the other hand, some devices that are designed for tapes actually stream the tape through the degausser to assure that the complete surface of the tape is cleared.

The strength of degaussers, and the coercivity of magnetic media vary quite widely. As tapes and drives are able to handle more data, it also becomes more difficult to erase them using a magnetic field. It should be verified with the manufacturer that a particular degausser is designed to handle the specific media that is to be erased. Be aware that most manufacturers are mainly concerned with the ability to prepare the media for reuse, and not necessarily make the data unrecoverable. The degausser needs to have at least 5 times the Oe value of the media in order to sufficiently destroy the data and to be considered sanitized. The NSA has classified three types of degaussers to assure that classified information is totally removed from a media. Type I

degaussers have the ability to securely erase media of 350 Oe or less. Type II equipment can safely remove data from media of 750 Oe or less, and Type III devices can sanitized media up to 1700 Oe[4]. Any media rated over 1700 Oe requires physical destruction.

c. Physical Destruction:

In some instances, it is necessary, or maybe even most convenient, to destroy the physical structure of a material by burning, chemical de-composition using acid, or by use of disintegration equipment that produces particle matter smaller than that of an ordinary paper shredder. These solutions result in a material from which data is virtually impossible to read.

Organizations with the proper incinerators can destroy their media by burning. If this method is used, it is necessary to verify that all the media has been meticulously reduced to extremely fine particles.

An acid solution can be used to dissolve the media to destroy its physical composition. While this is a very effective solution, it requires personnel that are qualified to handle the acid, as well as the appropriate facilities with adequate ventilation and spill cleanup capabilities.

Paper shredders should not be used in the destruction of magnetic media because the density of recording can leave fragments that are large enough to pull data from. Knife mills, also know as data disintegrators, are shredder-like devices that create an output that is extremely small (NSA specification: 3/32 inch)[5]. While these machines are expensive, they do provide a thorough destruction of many varying types of media, such as paper, diskettes, CD-ROM, and cassette tapes.

2. Magnetic Media Types and Preferred Disposal Methods:

Every organization needs to assess the risks versus the costs associated with each disposal method. An evaluation of the level of sensitivity of the data and the sophistication of those likely to attempt to access that data needs to be made. Each media type has a recommended destruction of data for disposal that is fairly absolute. Data should be removed as thoroughly as possible within financial means of the organization to do so.

a. Diskette Disposal:

Diskettes are a very insecure media for handling data. They move in and out of an organization without anyone giving much thought to them. They are often just tossed away once the user is finished with it, or if it develops a problem reading from or writing to one.

Disposal and destruction of diskettes should be centralized within a corporation to assure proper removal of any confidential information. All diskettes should be cleansed before disposal regardless of what is thought to be on them, even if the data is seemingly harmless. This assures that any data that may have been deleted, but is still retrievable, is scrubbed from the diskette.

[4] NSA, p.1.
[5] San Diego ISAC, p. 9.

Any diskettes received from an outside source, should also be cleansed. This includes program diskettes, and any unsolicited mailings such as AOL that are not immediately thrown away; while, it is unlikely that these disks contain any confidential data when they arrive in the organization, they are often formatted, and used as blank disks to hold a variety of information.

The overwrite method or Type II degaussing can be used to clear a diskette for re-use. However the DoD recommendation for sanitizing is physical destruction by incineration or a data disintegrator[6].

b. Hard Drive Disposal:

When hard drives are upgraded or systems replaced, care must be taken in how the drive is cleansed before the hard drive is installed in a new system or is disposed. The same persons responsible for diskette disposal should handle all hard drives in a centralized manner. The task of cleansing these devices is similar to a diskette, although each drive will take more time.

Each drive should be evaluated on the criticality of the data that it holds and the likelihood of any confidential information being retrieved. For example, a drive coming out of a server that holds financial data for the corporation, may be considered more sensitive than a hard drive that comes from a maintenance worker's PC. This does not mean that the data from the maintenance worker's PC should be ignored, but it may not require as detailed a destruction procedure as the drive from the finance server.

Overwriting hard drives is the least expensive method of clearing a hard disk for both re-use and disposal. Care must be taken to assure that enough overwrites are properly performed so that the data cannot be recovered. Degaussing is also acceptable, but not recommended if the drive is to be re-used, because factory installed sync information could be wiped out. The aluminum casings that cover most hard drives will allow for proper degaussing because it does not conduct the magnetic field. The coercivity of most hard drives would indicate that they would require a Type III degausser to meet NSA requirements for sanitation[7].

c. Tape Media Disposal:

As tapes are retired from use, or fail, their disposal should be handled in a manner similar to diskettes, and hard drives.

Because of their high density, they require more time, and stronger methods of destruction need to be employed in order to make the data difficult to recover. In almost all cases, tapes carry a large amount of confidential information and therefore require a higher sense of urgency when dealing with their disposal.

Many organizations retain old tape formats, even after they no longer have the model of drive available to read them. As systems are updated, it is important to remember to move data from old technology to the newer

[6] Netsys, p.1.
[7] Gutmann, p. 10.

technology, so that there can be tighter controls on the data. Once the data has been moved to a different media, the old tapes should be disposed of.

Because of the time and effort an over-write would take, tapes are usually degaussed or physically destroyed before being disposed of. Most tapes in use today (DLT, 8mm, 4mm DAT, etc) require a Type III degausser in order for them to be purged properly. If physical destruction is used, it needs to be remembered that these media store data very densely; any residue left over should be extremely minute. If the tapes are going to be used again, the degausser needs only to have an Oe value higher than the tape media. Even though these are now considered "blank" tapes, they still should be treated as securely as an active tape. Since some tapes have sync tracks that would be destroyed if degaussed, this method of destruction should be verified with the manufacturer for tapes that are to be re-used[8].

3. CD-ROM and Optical Disk Disposal:

With the advent of optical disk media, and the CD-R, CD-RW and other similar CD-ROM material, comes the need to control the confidential information that may reside on them. Corporate policies should be in place to instruct users in appropriate creation and disposal of optical and CD media. As with most media, the disposal of this media should be centralized.

One popular way of destroying a CD is to place it in a microwave oven for about 5 seconds[9]. While this method may be adequate for some organizations, the fumes that are given off may not be that safe. There are many products coming on the market for that can be used for the proper destruction of the CD media, some which are very inexpensive. Some of these devices are available for as low as $40.00; they take some of the surface off of the CD. After the CD is run through this device two or three times, rotating the disk on each pass, it would be very difficult to retrieve any data off of it. This method is certainly as effective as the microwave method.

The NSA has approved devices that actually strip the data layer off of the CD, but retains the inner hub for identification purposes. These devices, which cost thousands of dollars, sanitize the disks. A suitably rated knife mill could, also, be used to destroy these disks.

4. Random Access Memory (RAM):

While, this is a very unlikely source volatility for most organizations, RAM can pose problems for smaller amounts of datasets such as keys.

After memory has had the same data stored on it in powered up state for hours, or even days, it can "remember" this data at the next power up. This is common in static RAM, but can also occur with dynamic RAM

One solution to erase the memory is to expose it to high heat (140C) for several hours[10], but this risks damaging the RAM. Some suggest that even this is not enough, and that the memory should be ground in a knife or hammer mill

[8] Peripheral Manufacturing, p.1.
[9] Haas, p.1.
[10] Gutmann, p. 15.

to make any possibility of recovery non-existent. In most cases, the memory can simply be taken out of the device, stored for several days, and it will lose the data stored in it.

5. Personal Digital Assistant Upgrades and Disposal:

In most organizations the personal digital assistant (PDA) poses a huge risk. These devices are often the personal property of the user, but they often contain data that belongs to the corporation. When the user decides to upgrade to a newer model, their old PDA gets passed down to an associate, spouse, or even to one of their children. Policies need to be put in place that not only deal with what can be loaded onto a PDA, but also how the device is disposed of or passed on to the next user.

Some organizations are starting to purchase PDA's for their employees in order to have tighter control over how they are used. Some are trying to keep confidential information off these devices, by setting policies against it. Even if the users adhere to these policies, many now use the devices to store passwords, and PIN's.

In most cases, if a PDA's battery is allowed to drain, the data will be sufficiently erased; this does take some time, however. There are programs available that will encrypt and protect the data on the PDA while it is in use. Some have features that overwrite the data, bit by bit, if too many incorrect password attempts are made, or if the PDA is not synced within a set period of time. While, this is convenient for the security of the data while it is in use, it also allows for a secure write-over of the data when it comes time to retire or pass on the device. It should be remembered that if data were written to flash memory, draining the battery would not clear it.

Like RAM absolute physical destruction is probably the only sure way to deal with these devices.

6. Digital Cameras and Flash Memory:

Digital cameras pose an unusual threat in that they are generally not thought of as devices that hold confidential data. However, in one case with which I have personal experienced, a user had taken pictures of some charts that contained sensitive data, and imported them into a PowerPoint presentation. While, she had concealed the sensitive data in the presentation, it still was residing in the memory of a camera. That camera is shared out among many individuals that are employed by the company. The person responsible for the loaning out of the camera discovered the pictures in question, and erased them before loaning out the device to anyone else. The person who had taken the pictures was sure that she had erased them. Sure enough, it happened to again, to another person who borrowed the camera, although with non-confidential pictures. There appeared to be bug with camera; it did not erase its flash memory reliably.

In another incident recently, a memory stick that held cancer patient data was repackaged and re-sold with data still intact[11].

[11] Leyden, p.1.

It is imperative that flash memory that may hold confidential data be properly erased or destroyed.

7. Video Displays, Copier and Laser Printer Drums:

Video displays can get images burned into them that contain confidential information. When this happens, the screen should be destroyed. This can happen even more often on the developer drum of a copier or laser printer. These devices should also be checked for proper destruction of the data.

Hughs, Gwen, “Destruction of Patient Health Information”, November 2002 http://library.ahima.org/xpedio/groups/public/documents/ahima/pub_bok1_016468.html (11 March 2003)

McKenzie, Matthew, “Caution: Data disposal can be hazardous to your health” May 2002 http://storagemagazine.techtarget.com/strgPrintFriendly/0,293813,sid35_gci821125,00.html (13 March 2003)

NetSys, “Excerpt of DoD 5220.22-M regarding cleaning and sanitizing of data” http://www.netsys.com/cgi-bin/display_article.cgi?1241 (24 March 2003)

Department of Defense, “National Industrial Security Program Operating Manual”, 30 April 1997 http://cryptome.org/nispom/nispom.htm (11 March 2003)

Genio Group USA LLC, “Data Destruction” http://www.geniousa.com/Customer_Relations/Products/Software/secure_delete/security_deleting.htm (11 March 2003)

Gutmann, Peter, “Secure Deletion of Data from Magnetic and Solid-State Memory”, 22 July 1996 http://www.usenix.org/publications/library/proceedings/sec96/full_papers/gutmann/ (11 March 2003)

Gallagher, Patrick R., “A Guide to Understanding Data Remanence in Automated Information Systems” September 1991 http://www.fas.org/irp/nsa/rainbow/tg025-2.htm (31 March 2003)

Rice, Jim, “Nanotechnology: The Homebrew STM Page”, 10 May 1996 http://www.bsc.ustc.edu.cn/~jlyang/research/STMWebPage.html (1 April 2003)

San Diego ISAC, “NSA-Approved Destruction Devices” 5 April 2000 http://www.sdisac.com/NDAdest.doc (24 March 2003)

Peripheral Manufacturing, “Degaussing Information” http://www.periphman.com/degaussing_info.html (2 April 2003)

NSA, “Magnetic Tape Degaussing”, 5 March 2001 http://www.dss.mil/infoas/magnetic_tape_degaussing.doc (11 March 2003)

“DoD Standards for Clearing and Purging Media” http://www.all.net/books/standards/remnants/standards.html (24 March 2003)

“How a Disintegrator Works” http://www.semshred.com/DisintegratorWorks.htm (3 April 2003)

Marquis, Duane, “Data Destruction Device Approved for CD-RW Destruction”, 1 November 1991 http://www.cdrominc.com/info/news24.asp (3 April 2003)

“PDA Defense Information” http://www.pdadefense.com/features.asp (24 March 2003)

Leydon, John, “For Sale: memory stick plus cancer patient records” 13 March 2003 http://www.theregister.co.uk/content/55/29752.html (24 March 2003)

Haas, Paul, “CD-ROM’s in the Microwave” http://www.hamjudo.com/notes/cdrom.html (11 March 2003)