DISPOSITION OF SENSITIVE AUTOMATED INFORMATION

CSL BULLETIN
Advising users on computer systems technology
October 1992

This CSL Bulletin discusses the sanitization of magnetic media used to store sensitive information and supplements FIRMR Bulletin C-22 on the security and privacy of federal information processing resources, issued by the General Services Administration on September 18, 1992. Sanitization means the removal of data from storage media so that, for all practical purposes, the data cannot be retrieved. Some instances in which sanitization must be considered include whenever media is transferred from one organization to another, when equipment is declared surplus, and when organizations dispose of media.

Much of the information in this CSL Bulletin was drawn from the National Computer Security Center's A Guide to Understanding Data Remanence in Automated Information Systems, (NCSC-TG-025, Library No. S-236,082, Version 2) which provides specific technical guidance.

Sanitization: Why Be Concerned?

In the past, reports have surfaced that federal agencies have disposed of surplus information technology (IT) equipment without taking appropriate measures to erase the information stored on the system's media. This can lead to the disclosure of sensitive information, embarrassment to the agency, costly investigations, and other consequences which could have been avoided.

Sharing of media within the government or between government and contractors also presents security issues. For example, IT equipment is sometimes transferred between offices without first removing sensitive files. Diskettes may be used to transfer documents or data files (e.g., for time and attendance reporting) between offices with little concern for the other information which may reside on the diskette.

Employees throw away old diskettes believing that "erasing" the files on the diskette has made the data unretrievable. In reality, however, "erasing" a file simply removes the "pointer" to that file. The pointer tells the computer where the file is physically stored on the disk. Without this pointer, the files will not appear on a directory listing of the diskette's files. This does not mean that the file was removed from the diskette. (Commonly available utility programs can often retrieve information that is presumed "deleted.") Fortunately, with foresight and appropriate planning, these situations can be avoided.

Specific Agency Policies

FIRMR Bulletin C-22 states that federal agencies must establish policies and procedures to ensure the proper disposition of sensitive automated information. Some factors to be considered in developing agency policies are:

- Magnetic media may be exposed to unauthorized access at various times in the system life cycle. When are exposures most likely to occur? How do these exposures occur? What types of data are at risk? What procedures are appropriate for disposal of media for the agency's specific operating environment?
- Contractors typically use their IT systems to process information owned by a federal agency. Are policies or contractual mechanisms in place to adequately protect this information? Contractors must be aware of the importance of implementing appropriate sanitization policies and procedures. Binding contractual provisions to ensure the protection of the agency's information are often appropriate.
- The agency's computer security training and awareness program can be an effective mechanism to address media disposal and sanitization issues. Users require specific guidance and a source of answers to their questions.
- Does the agency lease equipment? If so, leased equipment used to process sensitive information should not be returned to the vendor unless the media is sanitized.

Techniques for Media Sanitization[sanitize]

Three techniques are commonly used for media sanitization:

overwriting, degaussing, and destruction. Overwriting and degaussing are the methods recommended for disposition of sensitive automated information. (Users of classified systems may also have to be concerned with data remanence. This refers to the residual information left behind once media has been in some way erased.) Security officers should be consulted for appropriate guidance.

Overwriting

Overwriting is an effective method of clearing data from magnetic media. As the name implies, overwriting utilizes a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located. The number of times that media is overwritten depends on the level of sensitivity of the information. Overwriting should not be confused with merely deleting the pointer to a file, as discussed above.

Of course, in order for overwriting to be used, the media must be in working order; for example, overwriting may not be used on a disk which has suffered a head crash nor on a diskette which has had coffee spilled on it. Regular preventative maintenance can help keep drives in working order to minimize head crashes. Many programs are available, particularly for PCs, that have an overwrite function.

Although overwriting can be used for clearing magnetic tapes, this method is time-consuming and generally never used. Degaussing, as discussed below, is a better alternative.

In the design of sensitive applications, software developers may wish to consider integrating overwrite capability directly into the application.

Degaussing

Degaussing is a method to magnetically erase data from magnetic media. Two types of degaussers exist: strong magnets and electric degaussers. Degaussers are tested by the Department of Defense; those which meet their requirements are placed on the Degausser Products List (DPL) of the National Security Agency's (NSA) Information Systems Security Products and Services Catalogue.

Different types of degaussing magnets are appropriate for varying types of magnetic media; consult the NSA's A Guide to Understanding Data Remanence in Automated Information Systems for details. Note that common magnets (e.g., those used to hang a picture on a wall) are fairly weak and cannot effectively degauss magnetic media.

Destruction

The final method of sanitization is destruction of the media. NCSC-TG-025 provides specifics on this method and its applicability. Shredding diskettes, after removing the outer protective casing, is also an option for unclassified media.

Employee Training and Awareness

Most employees who utilize IT systems also use, and in fact are often the custodians of, magnetic media. It is therefore important for agencies to give the issue of media sanitization appropriate attention in the agency computer security training and awareness program.

Employees should understand the following essential elements:

- Media containing sensitive information should not be released without appropriate sanitization.
- File deletion functions (e.g., the DEL command on MS-DOS) usually can be expected to remove only the pointer to a file (i.e., the file is often still recoverable).
- When data is removed from storage media, every precaution should be taken to remove duplicate versions that may exist on the same or other storage media, back-up files, temporary files, hidden files, or extended memory.
- Media in surplus equipment should be sanitized.

Data Remanence

A term which often arises during discussions of magnetic media sanitization is "data remanence." Data remanence is the residual magnetic or electrical representation of data that has been in some way erased or overwritten. This

residual information may allow data to be reconstructed typically using laborious, time-consuming methods. This usually is a concern only to those processing classified information. For the unclassified community, overwriting of media is usually sufficient to reduce the threat of data reconstruction from data remanence. Often utility overwrite programs contain an option to overwrite the location of the file three times, ensuring that the chance of recovery of the information from data remanence is very remote.

Disk Encryption

Another approach to solving the problems raised in this bulletin is through the use of integrated encryption technology. This technology uses a device or software which encrypts all data as it is written to the disk. When the user retrieves a file, the data is automatically decrypted for the owner to use. This encryption/decryption process is typically transparent to the user. Should the disk be lost or stolen, no useful data can be retrieved without the legitimate owner's encryption key.

Other Technologies

While this CSL Bulletin focuses on the need for sanitization of magnetic media, users should be aware that other storage technologies (e.g., optical media, EEPROM, bubble memory, UVPROM) may require special procedures. Security officers should be consulted when such issues arise.

References

FIRMR Bulletin C-22, Security and Privacy Protection of Federal Information Processing (FIP) Resources, September 18, 1992. Issued by the General Services Administration.

NBS Special Publication 500-101, Care and Handling of Computer Magnetic Storage Media, June 1983. A general guide to preservation of data on storage media particularly magnetic tapes and flexible disk cartridges. Available from the National Technical Information Service, Springfield, VA 22161, as PB83-237271.

NCSC-TG-025, A Guide to Understanding Data Remanence in Automated Information Systems, Version 2, September 1991. National Security Agency, Ft. Meade, MD 20755-6000.

Degausser Products List of NSA's Information Systems Security Products and Services Catalogue, issued quarterly by the National Security Agency, Ft. Meade, MD 20755-6000.