5 Data Destruction Tips from NIST 800-88

The National Institute of Standards and Technology's recent update to the 800-88 Guidelines for Media Sanitization document focuses on categorizing media according to the level of confidential data stored on the media.

After an organization has a snap shot of the risks of a potential data breach it is then possible to determine appropriate data destruction tools, recording methods, and overall media disposition strategy. This paper breaks this very detailed document down to 5 critical tips for implementing a secure media sanitization and disposition program.

#1 Categorize Media According to Level of Data Confidentiality and Associated Risk

Categorizing an organization's media by data confidentiality level makes good sense for both an IT department's operating efficiency and overall data security strategy. NIST advises organizations to determine the level of confidentiality according to the risk of a potential data leak. Aside from fines and fees associated with leaking of confidential employee and client information an organization should weigh the risks of forfeited revenues from lost future business or expenses from unwanted disclosure of intellectual property and company strategy.

Once an organization has an understanding of the risks associated to each media category leadership can then determine the appropriate methods and attention required to institute a data destruction process.

For example an organization may feel specific media from a graphic design department is not a risk from exposure but that all of the accounting department's media should be classified as confidential. In this scenario IT leadership may opt to put less stringent policies into play for media from the graphic design department while placing a multi-step, verifiable, recorded, and certified data destruction policy in place for the accounting department's data. In regards to disposition leadership may direct physical destruction or data wiping (purging) according to the various levels of confidentiality assigned.

#2 Choose Data Destruction Policies According To Life Cycle Stage and Destination of Media

Once your organization understands the hierarchy of risk and has categorized media accordingly, data destruction policy can be driven by where the media stands in the life cycle stage. Media that is being transferred or put back into use in an organization may have a different data destruction standard than hard drives that will be retired and disposed of.

Your organization may choose to have highly confidential media physically destroyed on location prior to disposal, but for that same media approve data sanitization with verification for internal reuse. Verification and documentation of data destruction methods should be chosen according to the life cycle as well.

Selecting the type of destruction tool will also be driven by the media's life cycle stage. It may not be possible to reuse certain types of media that have been degaussed or otherwise physically altered. In certain instances an organization may choose to only reformat or "clear" media prior to reuse or transfer for lower confidential hard drives and electronic media. The reformatting or "clearing" methods should not be used for media of any confidentiality level prior to disposal. At disposal sanitization or destruction should be utilized.

It may not be necessary to document data destruction during internal reuse and transfers but prior to disposition an organization should require documentation and signature certification regardless of the data confidentiality level.

#3 Approve and Utilize Appropriate Data Destruction Tools for Each Type of Media

Organizations need to approve and obtain physical and software tools to perform various levels of data destruction. These tools can be managed internally or an organization may rely on vendors for certain functions, but either way the process needs to include steps to verify the success of tools.

It is necessary to maintain several tools as no single method will be universally effective. For example if data wiping or purging is a company's preferred method for all media the products available to do so may not be compatible with certain systems and platforms. Mechanical defects and bad sectors may also make secure sanitization impossible. In these cases a company should maintain a physical destruction procedure or magnetic degaussing option even though the organization may have approved data purging for confidential media.

Perhaps the most prudent example to highlight is the approved methods for Solid State Disk (SSD) data eradication. NIST's current document approves clear, purge, and destroy for SSD. It should be specifically noted that degaussing SSD does not destroy data on the disks as SSD do not utilize magnetic technology to store information. NIST goes on to highlight that sanitization and clearing SSD requires verification, manual checks by technicians that data has been cleared and typically speaking quality checks from management on implementation of overall process. There have been reports and studies on SSD data erasure that show although clearing and wiping tools may report success of data eradication paths to data may still be intact making verification a necessary step in a secure practice.

#4 Document Certification of Destruction During Media Disposition

A key feature to any data destruction and end of life media plan is to develop an auditable depository of information focused on capturing key details throughout the destruction procedures. NIST stresses the key items to note as follows.

- Confidentiality Level of Media
- Description of Destruction (Clear, Purge, Damage, Destroy)
- Method (Degauss, overwrite, wiping, crypto erase, shredding)
- Tool Used (include version, brand, make and/or model)
- Verification Method (Full manual check, quick sample etc.)
- Post erasure confidentiality level and ultimate destination
- Name of responsible person, title, date, location, and contact information
- Signature of Person

#5 Data Destruction Process Requires Verification and Quality Assurance Overview from Management

A secure data destruction procedure needs to include verification of data erasure via reporting tools built into available sanitization products as well as sampling and complete investigations to verify success of data erasure. IT leadership should also require management to oversee and provide performance evaluations and regular sampling of the work being performed. The amount of oversight, verifications, and quality assurance should again be dictated according to the confidentiality of the media and risk of a data breach or leak.