Re-evaluating Data-Destruction Policies

The recent events, surrounding the exposure of sensitive missile information on a used hard drive; suggest a review of corporate and organizational data-destruction policies. Lockheed Martin, with a policy of on-site data destruction, found itself in the unenviable position of exposing sensitive information regarding the U.S. Terminal High Altitude Area Defense into the public domain. This missile defense information was discovered on hard drives purchased through eBay. (http://www.upi.com/Top_News/2009/05/08/Used-hard-drives-contain-sensitive-data/UPI-22481241759678/)

This type of on-site policy, which is ubiquitous as a best practice, is failing organizations and is the reason why a review of data-destruction policies is needed now. How can esposure to both sensitive information and liability be prevented in the future, if companies already have a policy of on-site destruction? Let's look at a typical policy.

TYPICAL WORDING IN A DATA-DESTRUCTION POLICY:
(Taken from Stanford University web site)
http://www.stanford.edu/group/security/securecomputing/data_destruction_guidelines.html

Policies
The following three cases are intended to cover all possible circumstances during which data sanitization is required. In all cases, the device is assumed to contain prohibited or restricted data and is transferred within one of these three scenarios:

> ***Transferred within an Organization***
> *In this case, a computer or PDA is transferred from one person to another who works in the same organization and has the same level of access to prohibited or restricted data information. If the device is transferred to a staff member who has no permission to this prohibited or restricted data, the policy defaults to "Transferred to a Different Organization". As long as the original system owner and the new owner have the same rights to view the prohibited or restricted data stored on the device, there is no need for data sanitization. The system may be transferred without removing any confidential data. However if the recipient has no business need to access the stored prohibited or restricted data, the files containing this data should be sanitized according to the directions in the Sanitization Guidelines section.*

Transferred to a Different Organization
When a computer is transferred from one person to another in a different organizational unit, all prohibited or restricted data on the system should be sanitized, unless management representatives from both sides agree the recipient has rights to this prohibited or restricted data. Either the confidential data files or the entire disk should be erased according to directions in the Sanitization Guidelines section.

Device Disposal or Transferred Off Campus
When a computer is to be disposed of or transferred to someone not working for the university, all disks should be sanitized, whether or not they are known to contain any confidential data. No computer system should leave Stanford's control without all disks being either sanitized or removed. No disks, including flash memory devices, should be disposed of without being sanitized. PDAs (e.g., Palm Pilots, Pocket PC devices) and Smart Phones should have all data removed prior to being transferred to another person or being turned in for recycling.

PROBLEM
The problem with current on-site, data-destruction policies, such as the one outlined above, is that they require data erasure prior to being transferred, either inside or outside of an organization. While this policy sounds logical, it can result in systemic data loss into the public domain. Several of the most often cited causes of data loss during data retirement include:

1. Cannibalization
2. No communication of data destruction policy
3. No adherence to policy
4. No enforcement of policy
5. Negligence on the part of internal or outsourced resources

Heavy reliance on non-technical staff

Organizational dynamics contribute to sensitive data loss during IT retirement, especially among large enterprises. Many organizations have decentralized policies, and put the responsibility for data destruction at the department level. Other organizations have a centralized method, aggregating systems to an IT department for data destruction. Problems occur when systems get lost in transit, when non-technical personnel are relied on, and when technical staffs cannibalize quarantined systems. Organizations lose track of data once systems are removed from an electronic tracking mechanism such as a network.

SOLUTION
What is the solution? Networked devices account for the vast majority of systems with hard drives. These systems can be processed on-site and on-network, prior to de-installation. Moving the data-destruction policy upstream and enabling network administrators to erase data prior to network de-installation can eliminate the need for non-technical staff to perform erasure. It can eliminate data loss from cannibalization, lack of policy communication, lack of policy enforcement and general negligence from either internal or outsourced resources. Furthermore, any risk of loss during transportation can be eliminated, with the result being a centralized process with centralized authentication while chain of custody is kept within an organization.

What about encryption? A secure and useful method when sending systems to a third-party for data destruction, however risk of negligence on the part of the provider still remains as well as risk of loss during transportation. Cost-prohibitive is dedicated, point-to-point transportation. On-site and on-network data destruction continue to be a safer method and process.

What about shredding hard drives? Current overwrite technology delivers the same level of data destruction as shredding a hard drive does, but without the effects of destroying a reusable system. Keeping systems out of the waste stream and cost containment are important corporate responsibilities. Shredding a hard drive destines all or at least part of system to the waste stream. If recycled, all of the materials are not completely reused. Some materials must be discarded. If sold without hard drives, systems are typically not re-used in whole. Utilizing overwrite technology, making systems useful to the next person and keeping them out of the waste stream is an optimal solution.

Robert Davie • Founder – Venderis Software • rdavie@venderis.com • 919-656-7142