

## Weak PC Disposal Processes Hurt Security

By: Brian Prince

16 December 2010

*eWeek*

<http://www.eweek.com/c/a/Security/Weak-PC-Disposal-Processes-Hurt-Security-243091/>

### **A recent NASA audit underscored how weak IT asset disposal policies can endanger your company's data.**

Protecting PCs doesn't stop when they are still being used by employees; it continues to the very end of a machine's life—the day when it heads to the dump.

This was underscored recently by a NASA audit that revealed a number of security failures connected to machines slated for disposal. At NASA's Ames Research Center in California for example, there was no "sanitation verification testing" for PCs at the end of their life cycle. The situation was found to be the same at the Lyndon B. Johnson Space Center in Texas.

And the audit also found that 10 computers from the John F. Kennedy Space Center in Florida had been released to the public despite failing sanitation verification tests—meaning they had not been properly wiped. Four other computers that failed the tests were confiscated by the auditors when they found the machines were being prepared for sale or release to the public.

"When we tested the confiscated computers, we discovered that one contained data subject to export control by the International Traffic in Arms Regulations (ITAR)," according to NASA's report (PDF).

While compliance regulations touch on the secure disposal of machines, there is sometimes a disconnect when it comes to best practices for hardware that is being actively used versus systems that are taken offline, Todd Johnson, vice president of operations at Kroll Ontrack, told eWEEK.

"Enterprises typically are not concerned with the hardware that has been replaced because it is assumed that it does not have any real usefulness anymore," he said.

"I do not believe it is laziness, but rather that when compared with other items on an enterprise IT administrator's plate, the proper disposal of old hard drives is nearly always going to be at the bottom of their 'To-Do' list," Johnson added.

In a recent survey, the company found that 49 percent of respondents said their organization regularly erased data when disposing of computers. Thirty-percent said no, while 21 percent weren't sure.

"Organizations need a defined process of managing systems from deployment to retirement, but oftentimes there are gaps," Johnson said. "First, in the starter/leaver process, IT usually does a good job in deploying antivirus and encryption software when an employee starts; however, when they leave, the process to wipe that drive may not be there. The leaver process tends to be a

more involved process, and a path needs to be followed to be sure that all the data is actually wiped. ... IT teams are so strapped, they are always putting out fires, and because their plates are so full, they may just put old computers on a shelf and forget to wipe them."

A comprehensive IT asset disposition (ITAD) strategy should take into account all traditional data center and distributed IT assets as well as related equipment such as copiers and printers, according to an October 2009 report on the subject by Forrester Research. In the report, the analysts advised businesses to take a number of criteria into consideration when evaluating ITAD service providers. At the top of Forrester's list were items ranging from security practices to environmentally responsible disposal to the limits of liability protection.

"Most organizations will find it reasonable to simply destroy all storage media when it has reached the end of its operational life; storage media is cheap and effective controls are simple," said Sean Bruton, director of security at NeoSpire. "Many paper shredding companies provide these services. Some of them will even destroy your old hard drives, tapes and CDs on-site while you watch."

Federal agencies, he added, are required to have controls covering the secure destruction of information systems through compliance with regulations like the Federal Information Security Management Act.

"The fact that NASA willingly released computers without proper sanitization could point to a very common issue within organizations—security is not viewed as a pervasive and necessary part of operational planning, which results in discrepancies between the corporate security policy and the actual procedures being executed daily," Bruton said.