Experts: Data Security Paramount When Retiring Tech Assets

Brian Heaton | March 11, 2011

As government agencies look for ways to bolster revenue on a tighter budget, selling retired surplus computers and other devices has become a common practice. However, states that lack effective data erasure standards are leaving themselves vulnerable to security breaches, experts said.

Deleting old files and reinstalling operating systems may be sufficient for home users, but prepping a data-sensitive government device for sale, or returning one once a lease is up, involves thorough data erasure to ensure security. Solutions range from electronically “wiping” hard drives clean to permanent destruction of a device.

While businesses and agencies of all sizes typically have policies governing where retired equipment goes, many lack similar guidelines on how to handle the sensitive end-of-life data security issues with computers.

The end-of-life data security issue surfaced the week of March 6 when surplus computers in New Jersey that were marked ready for sale were found to contain personal and confidential government information, according to a state audit.

New Jersey did have erasure rules in place, but the policy wasn’t effectively enforced, experts said.

“It is a lack of oversight on implementing the policy,” said Frank Milia, vice president of account management at the IT Asset Management Group. “A lot of times, the disposal of equipment is the project you put the ‘green’ guy on.”

Ed Stukane, chief marketing officer of PlanITROI, an IT asset disposition company, said, “Part of the challenge is the whole idea of IT asset disposition has evolved, particularly over the last five years. Before, the idea of taking care of equipment at the end of its life was probably an IT guy’s part-time task.”

New Jersey’s system of each agency being responsible for its equipment is commonplace in state governments, said Jason Raymond, engineering manager of Acronis Inc., a company with government clients that specializes in data protection software. The private sector tends to take a more centralized approach.

Barbara Rembiesa, president of International Association of Information Technology Asset Managers (IAITAM), said governments should begin to adopt a more centralized approach, similar to the private sector’s.

Rembiesa said knowledge about best practices in the public sector is becoming more common.

“We do a lot of onsite training for government agencies, so … the knowledge is there,” she said. “But [because] there is so much red tape in government, it is very hard for them to get the proper processes in place.

”Our best practice is a centralized technology asset management area that includes data security,” she said. “With government agencies, they tend to work independently. But if they brought it together, they could centralize a lot of processes that would save millions of dollars and lower their risk at the same time.”

Not Just Computers

Devices such as tablets, smartphones, copiers, printers and flash drives have added to the security challenges facing IT staff.

IAITAM purchased a copier that was used in a government agency and the first time it was turned on, sensitive government documents were found stored in it. Although Rembiesa would not reveal which agency had previously owned the copier, she did stress that IAITAM was required to turn over the documents.

“This happens quite a bit, more than people realize,” Rembiesa said.

Security Methods

The most secure option is total destruction of the hard drive or device. Companies transport drives to a facility and physically shred the drives, or in some cases, vendors will do it on-site in an office.

However, destructing the hard drive requires purchasing a new one to install in the old computers in order to feasibly sell them. To avoid that added cost, most technology asset managers opt for erasure software that “wipes” the drive multiple times, essentially overwriting it with blank code.

There is a plethora of software that meet the U.S. Department of Defense (DoD) Clearing and Sanitizing Standard, DoD 5220.22-M. Essentially the standard requires following a basic overwrite procedure that can be done multiple times.

“A lot of people say a minimum of three times wiping the drive is OK, but we stick to seven,” Stukane said. “If you can’t conform to those standards, then you need to remove and destroy the drive.”

However, there is a lot of gray area, explained Milia from the IT Asset Management Group.

“It’s not a clear cut rule,” he said. “There are software solutions out there that are approved by DoD and that is where the standard comes from. DoD is basically saying anything that eradicates the data to their specifications is fine, but their own policy is physical destruction.”

Given the varying opinions, Rembiesa stressed the need for technology professionals to employ due diligence as they create and implement end-of-life data security policies.

“My best advice would be to partner with a good disposal company and go over the standards,” she said. “Wiping [a drive] three or seven times doesn’t make much of a difference. It’s [about] how to best manage your IT assets to mitigate risk. That’s all it is.”

http://www.govtech.com/security/Experts-Data-Security-Paramount-When-Retiring-Tech-Assets.html