Legaltech news

Shredding Old Computers 'Into Dust' is the Best Way to Protect Law Firm Data

Disposing of old equipment isn't as simple as walking to the dumpster behind the office. It may cost law firms more than a hammer and a nail, but computer forensics has advanced to point where data on a decommissioned machine isn't truly gone until the hardware is ashes.

By Frank Ready | April 26, 2019

Photo by Leif K. Brooks/Wikimedia

"Gone, but not forgotten" isn't really a sentiment that law firms want applied to data that they thought was destroyed. Unfortunately, retiring old laptops, smartphones or other equipment is no longer as simple as picking up a hammer and driving a nail through the hard drive.

Frank Gillman, chief information security officer at Lewis Brisbois Bisgaard & Smith, noted that such an approach is popular among the do-it-yourself crowd. But he thinks that nowadays, people would be amazed at the data a talented forensic technician would be able to recover.

“If you’re not like literally shredding that stuff into dust, like the hard drive is going through a shredder with teeth and turning it into compost, it’s still dangerous,” Gillman said.

Raising the stakes somewhat is both the proliferation of data and the patchwork of global privacy regulations that have been enacted to prevent that data from being misused or imperiled. The European Union’s General Data Protection Regulation (GDPR) or the incoming California Consumer Privacy Act (CCPA), for example, both carry steep penalties for organizations that fail to safeguard the information in their care.

Gillman recommends that firms keep a detailed record of where particular pieces of information are being stored across internal devices. But even then it’s hard to account for every scrap of data a tool might encounter over the course of its lifespan. For instance, an attorney could enter a credit card number into a company laptop while making travel arrangements. “How do you know? And you really don’t,” Gillman said.

Still, once you’ve put the hammer down and slowly back away from the hard drive, don’t just pick an e-recycling company out of the phone book at random. Gillman suspects that most people don’t bother to look into the various methodologies employed by different providers.

Some e-recycling services might just overwrite a machine and call it a day, which can be effective but still not as foolproof as the aforementioned shredder with teeth. Opting to shred a machine could also buy firms leeway with regulators in the event that bad actors still manage to recover data from what’s left of the device.

“That’s what really protects you. You say, ‘Hey look, you know what, we did everything we could do,’” Gillman said.

There are also other steps that firms can take to help mitigate risk long before a given piece of equipment ever reaches retirement age. London-based law firm Bird & Bird discourages employees from storing data on hard drives, instead preferring that lawyers utilize its on-site document management system.

When data is loaded onto a portable machine as part of a presentation, for example, it's unlikely to be left there and forgotten. "We have a regular report that scans all local drives so we can track this," said Karen Jacks, IT director at Bird & Bird.

The firm also deploys a global policy for the disposal of equipment that includes the deletion of data using multi-pass pattern wiping before the device is sent to a certified specialist to be wiped and destroyed.

Having those types of procedures and protocols in place can go a long way towards mitigating human error or even just plain ignorance. Iliana Peters, a shareholder at Polsinelli, thinks it's important for employees within an organization to at least understand the process in place at their organization for the disposal of obsolete equipment. Even if the average worker doesn't know that a flash drive should be destroyed after use, chances are the IT department can take care of that for them.

"I think that law firms have to understand that their risk from a business associate standpoint when it comes to security is high," Peters said.