10 things you should do to securely dispose of computers

Takeaway: The need for good security practices doesn't go away just because a system has outlived its usefulness. These tips will help ensure that decommissioned equipment doesn't pose a threat.

Even in the best of times, computers are rotated out of use and we have to figure out how we should dispose of them. In a recession economy, people get laid off, systems running software with high licensing costs are decommissioned, and system breakdowns lead to consolidation of functionality rather than repairs. This may increase the rate at which we dispose of computer equipment — and it can increase the expose us to security threats if we aren't careful about how we do it. Take the following list of tips for secure equipment disposal to heart.

1: Eliminate access

Ensure that you eliminate any accounts or other access control facilities that are associated with the decommissioned equipment. You don't want an ex-employee still getting into his old workstation after he's not supposed to have access to it any longer, and you don't want lingering network access accounts used to remotely connect to the computer providing more "target surface" for security crackers when you don't need the account at all any longer. You should generally do this *first*.

2: Destroy the data

Don't assume that taking hard drives to the landfill is secure. If there's sensitive data on your drives, you need to get rid of it before taking it away. Even if you don't think there is any sensitive data on the drive, consider whether you're willing to bet the business on that — and if not, do more than just chuck the drive in the trash. Even reformatting or repartitioning a drive to "erase" the data it stores isn't good enough these days (if it ever was); tools such as the shred utility can help you delete files more securely. Encrypting the data on the drive before doing any deletion can help make data even more difficult to recover later.

3: Destroy the device

In the most extreme cases, storage devices may need to be physically destroyed to ensure that sensitive data isn't leaked to whoever gets the drives next, even within your own organization. In such cases, you probably shouldn't destroy them yourself. There are experts who can do this, and they're probably a lot better at safely and effectively rendering any data on your drives unrecoverable than you would be. If your needs are so stringent that you can't trust this to an outside agency that specializes in secure destruction of storage devices, you should have a specialized team within your organization that has the same equipment and skills as outside contractors.

4: Be methodical

Keep a checklist for the decommissioning process to make sure you don't forget a step at any point. This can be especially important when dealing with many, many computers at once, such as when an entire department is shut down — but it's important the rest of the time, too. Don't rely on the checklist to do your thinking for you, though. Consider every detail of the system in question, its uses, and any potential dangers for security that come to mind. Add new measures to the checklist when you come up with a threat you have to deal with that may be relevant again at a later date; not everything on the checklist has to apply in every case for it to be a valuable addition to the checklist.

5: Keep track of which systems have been decommissioned

Make sure you have clear, *physical* indicators of whether a system has been fully decommissioned in a secure manner and that they don't consist of something easily misplaced or overlooked like a sticky note. It's best if computers that haven't been fully decommissioned are kept in a specific location, while decommissioned equipment goes somewhere else, so that habits you develop will help you avoid making mistakes. For instance, perhaps workstations should be kept on desks and servers in racks until they're cleared (and they should probably stay there until they've had their drive contents shredded, at least, because they're already set up with power and whatever interface is normal for that system). Doing so can lend a sense of urgency to the need to securely decommission the equipment, too, because you'll feel the pressure of wanting to clear the space for other uses.

6: Keep careful records

Whoever is responsible for decommissioning a machine should sign off on the completion of the process if more than one person might be assigned such a responsibility. That way, if something goes wrong, you know who to talk to when it comes time to find out what happened and how bad the mistake really is. Log the time and date of completion, too. Just keep meticulous records in general, including the specifics of equipment components that have been processed, where they're going from here, and (when appropriate) their depreciated value and replacement cost.

7: Don't wait

Don't *store* equipment in need of secure decommissioning. Make it a priority to get it done, so the equipment doesn't end up being neglected for weeks, months, or years, until someone gets an opportunity to compromise your security by making use of sensitive data stored on it. Don't leave it running unnecessarily, either; you don't want yet another system running on your network, waiting to get compromised by a security cracker or malware, when you don't actually have any use for the system.

8: Eliminate potential clues

Clear configuration settings on networking equipment. Managed switches, authenticating serial console servers, and other "smart" network infrastructure devices can provide clues to a clever security cracker on how best to break into your network and the systems that reside on it.

9: Keep systems secure until disposal

Establish clear guidelines for who should have access to any equipment in need of secure disposal and track a "chain of custody" so you'll be better able to ensure nobody who shouldn't have access to it before disposal won't get his or her hands on it.

10: Inventory all equipment

Track the physical contents of every computer and piece of network infrastructure equipment in your organization so you won't make the mistake of overlooking a storage device. Remember that even volatile RAM can serve as a "storage device" for sensitive data under limited conditions. Ultimately, you should just adopt an attitude of practical paranoia about sensitive data storage and act accordingly.

Don't fall into the trap of meticulously securing your running systems, then getting compromised or having sensitive data recovered because you didn't put any thought into securing the systems slated for disposal. The need for good security practice doesn't go away when you turn off the computer.