

IT asset disposal: Are you prepared to pay the price?

According to the International Association of IT Asset Managers (IAITAM), 74% of companies felt risk reduction by securing data throughout the IT Asset Disposal program was extremely important. If company assets are found in the wrong place or found with company data, the directors will have to pay a hefty price.



Photo by Peignault Laurent on Unsplash

Many companies opt for in-house data destruction so they can destroy the hard drive themselves. Hard drive overwriting and degaussing followed by drilling, shredding, or breaking are common internal methods of data eradication used by these companies.

These methods can eliminate the upfront costs when compared to outsourcing this service, but as server rooms continue to grow, information continues to be stored across multiple platforms, and regulations continue to develop, outsourcing may be the only option when handling the destruction of data in greater volumes.

Xperien CEO, Wale Arewa, warns that it is imperative to work with qualified disposal vendors. "It is important to realise that although you can easily outsource recycling, you cannot outsource responsibility. Even diligent businesses are vulnerable to mischievous insiders and irresponsible vendors."

Adopt a formal ITAD policy to mitigate risk

Organisations must adopt a formal ITAD policy to mitigate risk and in order for it to be effective, but establishing chain-of-custody is far easier said than done. Preventing repercussions related to ITAD chain-of-custody requires a proven process and independent verification.

"Chain-of-custody controls must be established and should be monitored by an independent third party. When outsourcing ITAD to a qualified vendor, it is critical to establish a system of checks and balances. A chain-of-custody is required to shield your company from malicious insiders and downstream liability," he explains.

Arewa says insider crimes are by far the biggest threat and often go undetected. "Employees taking retired laptops for personal use are a common phenomenon. When a loss is detected, they can often escape responsibility by denying any knowledge or when caught red-handed, they tend to dismiss the importance and downplay the risk."

The repercussions for a company-wide security breach might seem unimaginable at first glance but it carries with it the potential for theft of information, negligence, and a hefty fine, not to mention a PR nightmare. Although most companies do take measures to protect their data while in use, they often neglect this critical data after the IT equipment leaves the company to be recycled.



Database of 30 million+ South Africans leaked online, property group is culprit

Ilse van den Berg 19 Oct 2017



"Data can remain accessible even after the equipment is destroyed, which is why it's necessary to work with an ITAD specialist who employs a thorough, certifiable data destruction process that wipes it completely and provides top quality security throughout the entire duration of custody of the equipment," he explains.

An ITAD specialist should carry certification that will hold the vendor accountable for practices that accord with environmental, security, and quality assurances. A vendor who is not certified is not likely to be fully compliant with regulations, which could potentially cost their clients as well.

One consideration that will benefit a company considerably is whether the vendor can provide a high-value return on the equipment being recycled.



Your IT needs a wake-up call - maybe PoPI is it

Pieter Engelbrecht 13 Oct 2017



"Why entrust decommissioned IT equipment with any vendor, who may also lack the security and certification measures, whilst there is the prospect of receiving a substantial return on the investment from a reliable ITAD specialist?" he asks.

Planning an IT asset decommission should include a value return, this makes planning the upgrade more robust and flexible. A certified ITAD specialist will have the skills and resources to provide the return.

"For maximum data security, regulatory compliance, and return on investment, it's critical to research and establish a working relationship with a reliable ITAD professional," he concludes.