The Five Most Common ITAD Mistakes (And How to Avoid Them)

Some say that the only certainties in this world are death, taxes — and managing obsolescence.

At least, that's what any IT specialist will tell you.

Organizations constantly replace outdated computers and other electronic devices to keep up with technology and enhance productivity. This rush to upgrade, however, creates a challenge due to the large number of electronics that must be managed and disposed of properly.

IT asset disposition (ITAD) is the process of responsibly retiring unwanted information technology. This includes transportation, equipment testing, data destruction, remarketing, de-manufacturing, recycling, and reporting.

Outsourcing these activities is easy. However, properly managing them is *much* harder.

When an organization fails to manage ITAD effectively, it becomes exposed to legal risks, environmental concerns, and unnecessary costs.

Here are five mistakes most organizations make that undermine ITAD efforts and expose them to unnecessary risk and avoidable costs:

1. *Not* using Third-Party Verification (TPV) to prevent problems before they happen
2. *Not* using disposal tags to deter theft and establish chain of custody
3. *Not* destroying or securing data before a move
4. *Not* getting competitive bids to maximize value and promote excellent service
5. *Not* auditing all bills and settlement reports

The good news is, avoiding these mistakes is easy. An ounce of prevention is worth millions in cure, and the payoff can be huge.

1. Use Third-Party Verification (TPV) to Prevent Problems *Before* They Happen

To err is human. But it's also expensive. Human error was responsible for approximately 90 percent of data breaches in 2019[1].

[1] Venafi blog referencing a CybSafe analysis of data from the UK Information Commissioner's Office (ICO); https://www.venafi.com/blog/7-data-breaches-caused-human-error-did-encryption-play-role

Internal ITAD activities are often performed by employees who are given little or no guidance from senior management. Why? Unfortunately, it's because the common view in ITAD is that a little inaccuracy saves a lot of explanation.

However, the fact is that leaving equipment disposition processes to one employee opens your business to potential theft, fraud, or worse.

Third-party verification helps prevent these issues. Not only that, TPV allows you to hold a vendor accountable should one occur.

Don't Let the Fox Watch the Henhouse

Data security laws mandate organizations implement measures that have segregation-of-duties or dual control. Dual control is essential because serious conflicts-of-interest exist.

However, the overwhelming majority of US companies rely on employees to work directly with electronics recyclers. This fails to meet the basic but critical segregation-of-duties requirement outlined in every major data security law.

Sadly, there is a huge incentive for recyclers to hide losses. And employees are no different. People naturally avoid reporting facts that could make them look bad.

In other words, these companies are allowing the IT fox to watch the ITAD henhouse.

When an organization fails to maintain proper oversight, outsourcing provides a false sense of security. That's why it's important to establish an independent set of checks and balances to mitigate risk and ensure compliance.

TPV Helps Hold Employees AND Vendors Accountable

A critical aspect of every major data security law is that organizations must minimize conflicts that create opportunities for theft and fraud. The focus to date has been on access privileges (for example, if an employee has the ability to cut themselves a check without authorization), but inherent conflicts-of-interest exist with ITAD programs as well.

Many IT professionals don't want the added responsibility of asset management. Some also have an incentive to avoid detection because they could be exposed for actually benefiting from this security gap. IT professionals are most often the direct beneficiaries of lost or misplaced items.

When an organization implements a process to validate chain of custody, it creates accountability. Losses can't be swept under the rug. Employees can no longer claim they didn't know equipment went missing. And they can no longer blame the electronics recycler (unless, of course, it truly is the recycler's fault).

Speaking of recyclers, organizations often rely on a vendor to document what was disposed of. Vendors shield themselves from liability by not providing complete and accurate information. Naturally, vendors want to avoid providing a "rope" to hang them.

It's important to recognize that the liabilities associated with ITAD are not revealed in what a recycler reports. The real risk results from what is *not* reported.

Third-party verification is already required in many industries. In light of the issues above, it's no surprise that it's becoming mandatory in ITAD as well.

2. Use Disposal Tags to Deter Theft and Establish Chain of Custody

The Risk of Relying on Serial Numbers Alone

On my dentist's wall, there's a clever sign that reads, "You don't have to floss all your teeth, just the ones you want to keep."

When it comes to ITAD, it's wise to remember a similar expression, "You don't have to tag all of your assets, just the ones you need to track."

Unbroken chain of custody is necessary to indemnify an organization from the downstream risks associated with ITAD. Typically, chain of custody is established by manually matching manufacturer serial numbers captured on a vendor inventory.

Sounds easy, right? Think again.

In a multi-year study of tracking data, only 47% of serial numbers captured could be matched successfully. In other words, relying solely on serial numbers to track chain of custody only leads to about a 50/50 chance of success.

With your company's reputation (and future) potentially on the line, do you really want to rely on those odds?

Disposal Tags Increase Tracking Accuracy from 50% To Nearly 100%

There's a reason airlines tag luggage and furniture movers tag boxes; it works.

Disposal tags are a far better way to track assets compared to serial numbers. Instead of a 50/50 chance, disposal tags increase accuracy in tracking to over 99%.

But that's not the only benefit disposal tags offer. They also deter theft. After all, employees are less likely to steal an asset they know will be missed.

Most importantly, disposal tags are your best tool in establishing a clear chain of custody for your retired equipment — something that serial numbers alone can't provide.

Simply put, tags are an easy yet highly effective way to prevent problems, save money, and streamline ITAD.

3. Destroy or Secure Data Before a Move

When it comes to data risk, it's best to cut the tail off at the neck. Theft of retired equipment that contains confidential data can be catastrophic.

Assign an employee to ensure all data is removed from a device as soon as it has been identified for disposition. The longer retired equipment is allowed to linger, the greater the chances that valuable data could end up in the wrong hands.

Utilize erasure software to fully destroy data on a disk. Non-working drives should be removed and physically destroyed using a hard drive crusher or even a hammer. Most importantly, data destruction should be documented.

In all cases, it is wise to destroy sensitive data *before* equipment leaves your facility. A driver could easily steal a computer containing confidential information — resulting in millions of dollars in damage to your organization.

Understanding Vendor Liability

Should a computer be stolen or lost during transit, a vendor might accept responsibility.

The key word here is *might*.
However, even if they did, it would be a hollow victory as the Carmack Amendment allows carriers to limit their liability for loss or damage to goods. That means you can't hold carriers responsible for breach of contract or negligence if they lose or damage your goods; you can only sue carriers under the terms of the Carmack Amendment.

You can outsource recycling, but not responsibility. That's why data stored on retired equipment should be destroyed before handing it off to a qualified IT asset disposal vendor. If you think a pretty certificate will protect you, think again.

Compliance and indemnification require unimpeachable chain of custody evidence. It's important to remember that unless you prove a vendor has your equipment, there is legal exposure. Disposal tags can protect you from that vulnerability by establishing clear chain of custody with a disposal vendor.

So why not ask a vendor, who is handling the equipment anyway, to also wipe data from the hard drives? You should. However, this should not be the primary method of data destruction. A vendor's data destruction services should be considered a secondary precaution. Remember, a vendor can't wipe data from a hard drive it never received.

4. Get Competitive Bids to Maximize Value and Promote Excellent Service

A little competition goes a long way.

When I joined the industry 20 years ago, most remarketing happened on a consignment basis. Revenue share arrangements took the guesswork out of getting a fair deal. Reports showed the actual sale price of equipment, there was total transparency, and incentives were aligned.

Fast forward to today, and most remarketing now happens on a Fair Market Value (FMV) basis. FMV is meant to be an accurate assessment of what a piece of equipment would sell for if sold today.

However, service providers have ultimate control as they set the value for the equipment they buy from you — meaning FMV is anything but fair.

The main problem with FMV is that it is a completely made-up number. It tends to be the lowest price a service provider thinks you'll accept before looking elsewhere. It's no wonder that some in the industry refer to FMV as *Fake* Market Value.

Relying on one vendor typically means leaving a lot of money on the table. Moreover, it can lead to unnecessary risk and subpar service.

How a Multi-Vendor Approach Protects Your Business

It's often tempting to go with a single vendor. You have one throat to choke, right?

But anyone involved with ITAD knows how once-trusted vendors can become unresponsive, get acquired, get into trouble, or simply go out-of-business.

What if...

- You catch the vendor in a lie?

- The vendor has a scandal?
- The vendor suffers a data breach?
- The vendor short-changes you on remarketing?

Countless issues can happen when vendors fail or let us down.

- Reports, records, and certificates get lost. Historical evidence that equipment was disposed of properly disappears.
- Unwanted equipment piles up. Stockpiling equipment requires space and increases exposure to employee theft and depreciating resale value.
- RFPs take time. Due diligence is required. Hurried decisions lead to worse problems down the road.

At first, your vendor is eager to please. Things go well for a couple of projects, but then your projects seem to take a backseat to the vendor's other affairs. The nice people you first started working with move on or are put on other accounts. After a while, you catch yourself making excuses for your vendor's lack of efficiency and feel grateful when they manage to perform basic services.

So, what's the solution?

ITAD is a process. And like any process, a single point of failure is risky. Your ITAD process should not change when you switch vendors, decide to work with multiple vendors, or when your once-trusted vendor goes out of business.

That's why the most effective strategy for ITAD success is a multi-vendor, vendor-neutral approach

5. Audit All Bills and Settlement Reports

Here's a scary statistic: approximately one-third of invoices from ITAD vendors contain errors.

Now, how often are these errors in your favor? You probably already guessed; few times, if any.

ITAD is often an unbudgeted expense in most organizations, so a common goal is "Breakeven or Better."

By that measure, achieving success should be easy. Reselling equipment can help offset the cost of IT disposal. If managed properly, it has the potential to generate significant returns depending on the age and condition of each piece.

However, no matter how valuable your used equipment, money will be left on the table if the IT disposal vendor fails to record the correct information about your equipment.

Where Vendors Fall Short on Equipment Remarketing

While some ITAD vendors have the mindset that "what a client doesn't know will benefit me," most are not maliciously trying to deceive their clients in terms of fees.

Instead, extra costs can be attributed to employee error. Account managers rarely audit reports, making it common for extra charges (sometimes for other's equipment) to appear.

Some ITAD vendors play games with remarketing. Others make honest mistakes. For example, if a vendor lists an item for sale on eBay with an incorrect manufacturer model number, what would typically sell for $80 may sell for only $8.

Compounding the problem, many vendors don't recognize they have an issue. And those that do often discount the size of the issue because they have no way of policing it.

In fact, most vendors do not have the controls in place to protect them from their own employees, past and present.

There is a cottage industry of dealers made up of former employees of IT disposal vendors who understand the true value of retired assets. They buy equipment from their previous employers and then resell it to dealers or end-users at a considerably higher price.

Bottom line, if you don't audit settlement reports, there is a significant chance your equipment is selling below fair market value and leaving you with less money than you're owed.

5 Mistakes — 1 Solution. Retire-IT is Your Partner in Solving Common ITAD Obstacles.

When it comes to ITAD, you can outsource tasks, but not responsibility.

When an organization makes mistakes managing ITAD, outsourcing ends up increasing risk and obscuring costs, all while providing a false sense of security.

That's where Retire-IT comes in.

We help companies avoid the five most common ITAD mistakes others make by:

- Supplying you with vendor-accepted disposal tags to easily track equipment, deter theft, and establish clear chain of custody.

- Connecting you with trustworthy ITAD vendors to ensure you receive top-dollar for your remarketed equipment.

- Providing cutting-edge technology to help you track and audit equipment across its entire lifespan and ensure that data is destroyed before disposal.

Remember, by avoiding these five mistakes and instituting simple ITAD policies, you can ensure your sensitive data is safe from the time a computer is deployed until the day it is retired.