WE DO ITAD RIGHT

Lifespan

10 Myths About ITAD Data Erasure

Overview

Data security is a top priority for most organizations for the disposition of their IT assets. Sensitive data must be cleared from the drives of retired IT equipment before it can be remarketed. However, many misconceptions exist about the process, standards and technology related to data erasure. The following document will shed some light on the data erasure process, dispelling some of the most common myths and discussing the best practices for optimizing your organization's ITAD program in this area.

You will find that by taking advantage of the latest techniques and technology, and by partnering with a vendor that is current with the latest industry standards, you will be able to minimize the risk to your organization of data loss and maximize its return on investment (ROI) for retired equipment.

WE DO ITAD RIGHT
Lifespan

It's cheaper to do it myself.

Commonly held belief that since you have staff who should know how to do a data erasure, then you should just use them and not pay a third party.

Truth While many organizations believe it's less expensive to permanently erase data from IT equipment in-house than by partnering with an asset disposition solution provider, some thoughtful review reveals costs that may be overlooked. Consider what your organization pays its technicians and the value of the time it takes them to set up, perform the erasure, and document it. There's also the opportunity cost: the cost of taking your team away from a project that may be more strategic for your organization. Finally, there are costs associated with the space, systems, and software required to perform data erasure. Make sure you consider all the costs.

Simple formula for calculating the cost of self data erasure:

Tech full cost hourly rate:

x (set up time, wipe time, document time).

x number of drives

+ QA (# drives x 5% x forensics test)

+ allocation for space, systems, erasure software licenses

+ cost of not completing some other projects on time/on budget

= TOTAL COST OF DOING IT YOURSELF

WE DO ITAD RIGHT
Lifespan

It is more secure to use my team than to outsource data erasure.

If the goal is to keep the data from getting out, then what better way than having our own people do it and not involve an outside company?

Truth

Security is the whole purpose for erasing data from retired IT equipment. Some companies reason that the best way to ensure total data erasure is to do it internally. That way, they have complete control of the process. Just make sure you have control over the process. Lifespan has found that as many as 10 percent of the drives it receives from clients who say they have erased the data on them still contain some form of data, either in remnant form or completely intact. For firms concerned about security, this is a major risk.

Your IT team may be skilled in several areas, but they may not all be familiar with proper data erasure procedures, either to perform the erasure or to check if it was successful. Busy IT staff members are also usually juggling several different tasks at any given time, so they may not be available to monitor the data erasure process to ensure quality from start to finish. Larger capacity drives can take an hour or more to properly erase. If you are using a disk-based tool, you must carefully check and document each device for a successful erasure.

Many times a busy staff is also lacking an adequate, dedicated space to perform the erasure process. This means that some devices or drives could get moved to the “erased” pile when they weren’t wiped at all, or when the erasure failed for some reason.

A staff dedicated solely to data erasure at a certified partner, on the other hand, will be trained in the process, software tools, standards and best practices. They can offer a documented data erasure process certified according to industry standards and they will not be distracted by other projects while they are serving your organization. The wipe can still be done onsite at your location – with a mobile wiping system, by that same certified process and staff.

WE DO ITAD RIGHT
Lifespan

Freeware works well enough for us.

I can download software for free for erasing drives – lots of people I know use it. Why pay for it?

Truth

You can't beat free for the cost of data erasure software. But free isn't always free when you factor in the loss of productivity from using slow and inefficient software, and the time it takes to manually document each drive that is wiped. Free software often comes from unknown sources and its creators may rarely, if ever, update it. You should also confirm that the software you use can erase all types of drives (SATA, IDE, SCSI, SAS, FC).

Another area of concern with free erasure software is that on modern hard drives, data can be stored in hidden partitions called Device Configuration Overlay (DCOs) or Host Protected Areas (HPAs).

From Wikipedia: The Device Configuration Overlay (DCO), which was first introduced in the ATA-6 standard, "Allows system vendors to purchase HDDs from different manufacturers with potentially different sizes, and then configure all HDDs to have the same number of sectors. An example of this would be using DCO to make an 80-gigabyte HDD appear as a 60-gigabyte HDD to both the (OS) and the BIOS... Given the potential to place data in these hidden areas, this is an area of concern…"

Most freeware tools won't see these partitions and will falsely report a drive clean when it still has data on it. Carefully review your data erasure tool's origins and documentation, and have a process to quality-check the results. The data stored on your retired IT equipment is too sensitive to trust to an unknown and untested software package.

Consider a commercially certified, documented tool that can support multiple devices on a LAN or in an array, and that will provide detailed reports electronically.

WE DO ITAD RIGHT
Lifespan

I trust the local vendor that I have been using for years.

We've never had a problem, and we like them and their service.

Truth

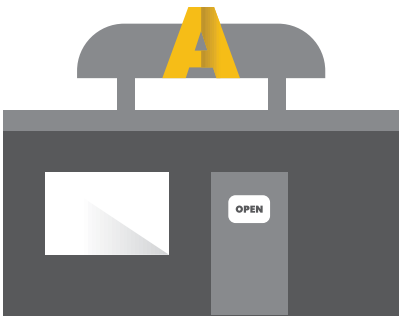
The risks are high. Make sure your trust is backed by knowledge and auditable records. How much do you know about your vendor? Have you observed your vendor's data erasure process? Have you visited its facilities? Do you know which data erasure tools it uses? Do you have reports that show every serial number and whether the erasure was successful or not? Have its employee's received proper training and background checks?

You may not have had any problems with your vendor yet, but it only takes one drive to get through the process with data still on it to cost your company a significant amount of money in fines and PR, and possibly stock price. The current average cost of a single data breach can be measured in thousands or even millions of dollars.

You should know what compliance and regulatory standards your organization must meet: HIPPA/HITECH, PCI, SOX, FACTA, GLB, FERPA – there are numerous regulations. Do you have an auditable record of your data erasures?

A data breach can also be very career-limiting.

If you use a certified IT asset disposition vendor, you can be sure that it meets the highest standards for data erasure and its entire disposition process had been documented. The National Association for Information Destruction (NAID) is one of the major certification bodies that focus exclusively on security, and it performs both an annual and a surprise audit each year on the organizations it certifies. By working with a certified ITAD provider, you're saving yourself the trouble of checking up on the work of your vendor, because it's already been done for you.



WE DO ITAD RIGHT
Lifespan

I am in full compliance with all state and federal environment regulations.

We turned our equipment over to a vendor to be recycled. Are they are in full compliance with environmental regulations?

Truth

When a drive can't be wiped (it won't boot, it's got damage and the software can't complete the erasure), what does your vendor do with that drive? It needs to be destroyed and disposed of properly, in full compliance with all state and federal environmental regulations. Again, a certified vendor can give you peace of mind here. R2 is an industry-sponsored standard, developed with industry support, to ensure environmental compliance and stewardship. Keep in mind that, even if you have turned over equipment to a vendor to be recycled, if the equipment has been disposed of improperly and if it can be traced back to your organization, your organization could be liable. Make sure any "certificate" of recycling is backed by more than just the paper it's printed on.

WE DO ITAD RIGHT
Lifespan

I am protected because I encrypt my drives.

We know our data is safe because we use encryption. No one can read the data.

Truth

While encryption is a good deterrent against those who try to access the data on your drives, it is not an accepted data sanitization industry standard in North America or Europe. That's because, although it's in a derivative form, the information is still there. The technology may not currently exist to access it in a commercially viable way, but that could change in the future as new techniques are developed. For asset retirement, proper data erasure will provide you with an electronic record that the encryption key and the encrypted data have been completely destroyed and no remnants remain – encrypted or not.

WE DO ITAD RIGHT
Lifespan

I destroy all my drives to be secure.

There is no data left if we physically destroy all the drives – it's the safest way. I know we've met the requirements if we do it.

Truth

The physical destruction of data-bearing hard drives can be satisfying and put worried IT managers at ease because it alters the drives beyond recovery in an immediately apparent way. However, all the major standards organizations in the U.S. and Europe accept proper data erasure as equal to the physical destructions of drives. So proper erasure = proper physical destruction.

IT assets without hard drives lose about 20 to 30 percent of their remarket value. The older the technology, the bigger the impact on value.

On the other hand, erasure does cost money, so erasing data from equipment that won't have resale value can be a waste. If the drive or asset is too old to have any remarket potential, the physical destruction might be a more time and cost-efficient solution.

One method—erasure or destruction—does not fit all the possible disposition scenarios, even within the same organization. A data center decommission, a laptop refresh or the shut down of an office with old equipment might have different risk/cost ratios. A good ITAD vendor can help you analyze the different factors and create a plan that balances your priorities regarding remarketing value, compliance, risk, and your security policy.

WE DO ITAD RIGHT
Lifespan

Solid State Drives (SSDs) cannot be erased.

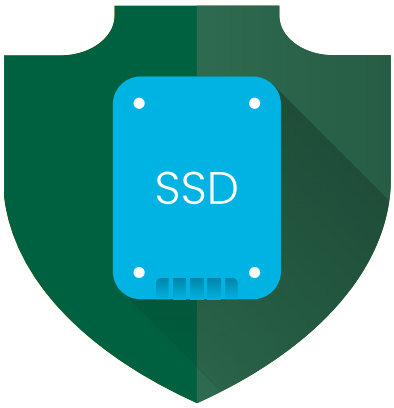
There is a lot of discussion about SSDs. Do we just need to destroy them when we are done with them?

Truth

Solid state drives have become a popular alternative to magnetic drives. SSDs and magnetic drives are the same in that you can write, read and erase data on them. Their underlying technology is quite different, however. Some believe data can never be fully erased from solid state drives. Experts at the University of California, San Diego Department of Computer Science and Engineering Non-Volatile Systems Laboratory (NVSL) have found that performing Secure Erase Enhanced (a data destruction command built into the firmware) can be effective if it's been implemented properly by the manufacturer.

There is no government standard that specifically addresses data erasure for solid state drives. Current industry recommendations are that the encryption key must be overwritten, then Secure Erase Enhanced should be requested if it is in the firmware, and finally a traditional overwrite done in such a way as to ensure the provisional cells in the drive are overwritten.

For more details on the underlying technology, erasure and security, contact Lifespan for a briefing based on our work with the UCSD NVSL and the NAID SSD Task Force.



WE DO ITAD RIGHT
Lifespan

I erased the drives, so I'm covered.

Our policy is to erase all hard drives. So we don't have anything to worry about.

Truth Simply believing data has been erased from retired equipment at some point is not enough to give IT managers peace of mind. Where is the equipment stored before erasure and where does it go after? With equipment coming and going and being processed through various stages of disposition, it's difficult to control the flow of equipment and monitor the location of a single piece of equipment at any given time.

Where is that asset from the moment the user relinquishes it until your ITAD vendor picks it up? Was it left in an open area? Did it get shipped by UPS or Fed Ex back to the main office (hint: not a secure process!). Where is the equipment stored before erasure, and who has access? How long is the equipment stored with data on it?

During the actual erasure process, what if the staff member is called away to a different task, leaving behind a stack of un-sanitized laptops which are then moved on to the next step by a different staff member – without confirming their erasure status.

Without a documented process and a clear chain of custody, there is risk that the equipment with data that hasn't been erased can slip through the cracks in the process and into the outside world. A well-documented disposition process is a necessity for any organization that is concerned about data security.

An ITAD service provider can help you assess your current program, identify gaps and find solutions that protect your data, minimize your workload and your costs. Much of this process is up to you – and you can ask experienced ITAD partners for best practices.

WE DO ITAD RIGHT
Lifespan

The Standard for Data Erasure is DOD (Department of Defense), Three-Pass or Seven-Pass.

We always get a "DoD wipe" on our drives. Our vendor is certified for that.

Truth

The Department of Defense standard for data erasure, DoD 5220.22-m, often referred to in the industry as simply "DoD," has been surpassed and incorporated into a newer standard. The latest U.S. government standard, developed by the National Institute of Standards and Technology and Homeland Security, is NIST 800-88. The previous DoD requirement of three passes is certainly effective. However, hard drive experts say that the 3 pass standard came about when the drive head accuracy was not very good. It took 3 passes to be sure that the entire drive had been overwritten. Modern drives write much more accurately than drives from 20 years ago and require only one pass to sanitize all data. Certified erasure software will do one complete pass and document the successful erasure. This is much more efficient, especially as the time to overwrite grows with the capacity of the drive.

Also note that in the US, the government does not "certify" any company for data erasure or destruction. The government backs a standard – NIST 800-88. A third-party certification body can ensure that the data erasure vendor you choose has processes in place that comply with the NIST 800-88 standard.

Resources:
NIST 800-88
Reliably Erasing Data From Flash-Based Solid State Drives
Center for Magnetic Recording and Research, University of California, San Diego
DoD 5220.22-M

01-2022

LIFESPAN INTERNATIONAL INC.

4675 E. Cotton Center Blvd., Ste. 155, Phoenix, AZ 85040 USA
951 Valley View Lane #180, Irving, TX, 75061 USA
75 Clegg Road, Markham, ON, L6G 1A1 Canada

Tel: (888) 720 – 0900
Email: info@lifespantechnology.com

WE DO ITAD RIGHT

Lifespan