TELLEREX

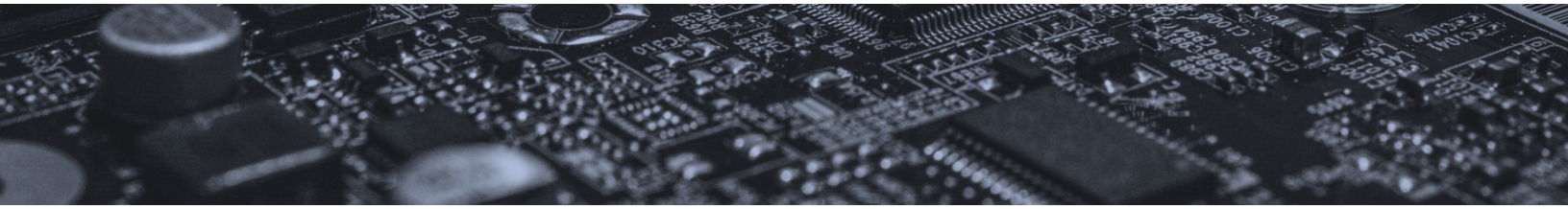
MITIGATING RISK IN ASSET DISPOSITION AND RECYCLING

Look anywhere, and you'll see thousands of articles and guides about preventing cybersecurity attacks. We all know the importance of trying to keep intruders out of your IT infrastructure. But what about the data safety risks when IT assets are retired and leave your organization?

Whether you're moving to the cloud, virtualizing your IT infrastructure, or doing a routine refresh or upgrade, every project will likely create surplus technology you'll need to remove from your work environment. IT asset managers must understand the issues involved in selecting outside vendors to guide and manage their organizations' IT asset disposal (ITAD) process.

Regardless of its function, most electronic assets manage data in some way, whether on a hard drive, flash drive, memory card, or another device. While this is not a new concept to consider, this dataset is often overlooked when it comes to the asset's disposal. In fact, a report from Deloitte found 33 percent of IT executives admitted having little or no formal IT governance policies in place for the retirement of their assets.

While data breaches often occur by bypassing network security remotely, physical attempts to steal locally stored data files are frequent as well. Physical data theft attempts occur whether devices are in use or prepped for disposal and recycling. There are a few areas throughout the e-recycling process where, without adequate security protocols in place, data can be at higher levels of risks.



DECOMMISSIONED ELECTRONICS ARE ONE OF THE MOST-STOLEN PRODUCTS.

> "Electronics recyclers today have to consider the secure transportation of equipment to their facility, and then how to maintain this security once it arrives and is prepared for further processing."
>
> - James Kilkelly
> President, Tellerex

ELECTRONICS ARE ONE OF THE MOST-STOLEN PRODUCT TYPES

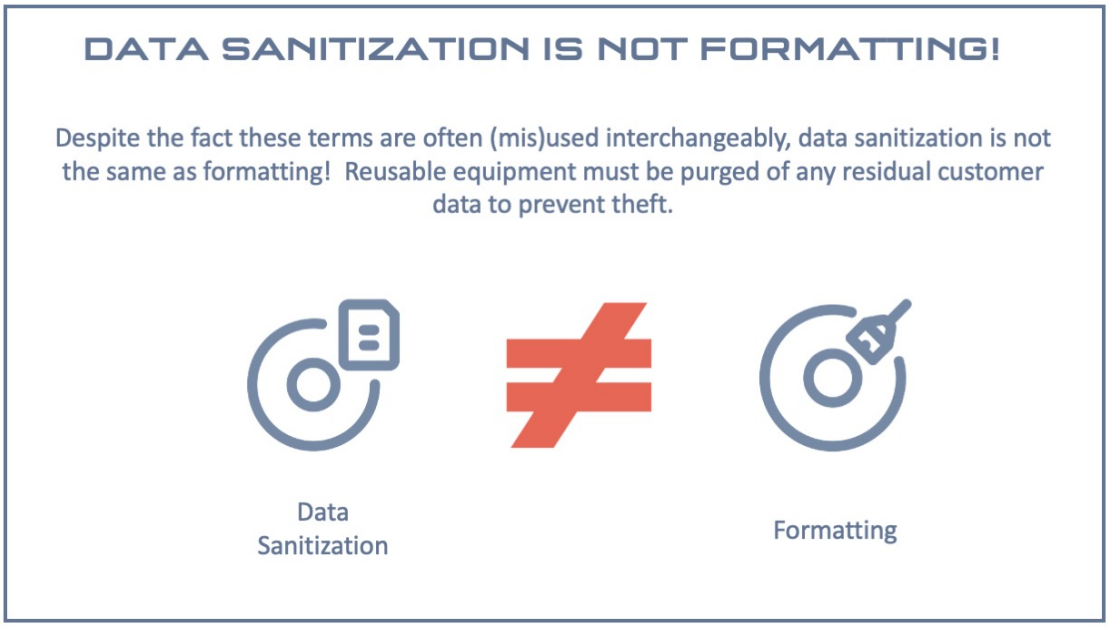
When it comes to cargo-theft specifically, electronics are among the top six commodities stolen globally.

66%
of electronic thefts happen while cargo is in transit

11%
of electronic thefts happen while cargo is in a warehouse.

A QUICK WARNING ABOUT DATA SANITIZATION CLAIMS

Despite the fact the terms are mistakenly used interchangeably, data sanitization does not mean formatting! Data sanitization is not the same process used to overwrite information on a hard drive.



The only way to ensure complete data sanitization is to completely remove sensitive data from IT assets before their destruction or resale. Unfortunately, the physical destruction of a hard drive, by either degaussing or shredding, is not infallible. With destruction, small portions of the hard drive may be left intact, and data recovery can still occur.

IN SOME CASES, DATA CAN BE RETRIEVED FROM HARD DRIVES SHREDDED FOR RECYCLING

Believe it or not, if somebody wants to retrieve data from a shredded hard drive, they can attempt to rebuild the drive from the shredded pieces. While their success is unlikely, it is still possible with enough patience and the right set of tools.

For this reason, extra consideration should be taken when evaluating data destruction and IT asset disposal services. Steps for data destruction might include:

- Erasing data (via degaussing) before the hard drive is shredded,
- Witnessing the data removal and destruction processes, or
- Reviewing security standards implemented and maintained by your recycler or data destruction partner.

These less secure methods, especially hard drive reformatting, expose companies to high risks of a data breach. Someone with the right skills will likely be able to recover most or all of the data on a reformatted disc. This fact is unfortunate, given a recent study, which found 34% of asset managers choose hard drive reformatting as one of the top-three most selected options to protect against a data breach.

ENSURE COMPLETE DATA SANITIZATION!

The only way to ensure complete data sanitization is to remove sensitive data from IT assets before their destruction or resale. Physical destruction, by either degaussing or shredding, is not infallible. With destruction, small portions of drives may be left intact, and data can be recovered.

Degaussing is an option for HDD devices, but only through the utilization of a high-quality degausser. If a company chooses this method, the organization must ensure that data sanitization is managed and adequately audited with a fully secure and visible chain of custody.

Reusable equipment must be purged of any customer data to prevent theft. The process for data sanitization should always conform to procedures outlined in NIST 800-88 Standard, NAID, ADISA, or R2:2013. This process should also include controlling security, record-keeping, and verification.

SELECTING A RESPONSIBLE IT ASSET DISPOSITION AND RECYCLING PARTNER

IT asset disposition partners (ITADs) must be knowledgeable about securely erasing company data that resides on "aged-out" assets – no matter the plan for the ultimate disposal of the equipment. This step is critical to the security of the ITAD's customers and partners. It's simply not enough to "wipe" the hard drive of a PC, laptop, ATM, or other IT assets. Full and secure data sanitization is critical to prevent security breaches and data leaks.

ITADs and recyclers who build and maintain robust security policies to safeguard sensitive data will set themselves apart from their competitors. Providing certification of secure erasure proves to customers that they can trust this process (and their ITAD partner) and that wherever aged-equipment ultimately ends up – destroyed, recycled, or reused – sensitive data will not be compromised or sold on the black market.

Among the areas where ITADs should be able to tout their expertise are:

- On-site validation of asset inventory.
- Packing and removal of equipment.
- Proper disposal of ecologically-sensitive materials.
- Donating unwanted equipment to charities or non-profits.
- Boosting an organization's social or environmental reputation.

ITAD PARTNERS SHOULD HAVE A ROBUST (AND AUDITABLE) PROCESS TO MANAGE DECOMISSIONED ASSETS

When working with a legitimate recycler, there should be an auditable procedure in place to dismantle devices, separate their components (including removal of any hazardous waste), and shred the materials into different materials.

Once shredded, the material should be separated again, with commodities of value sent to downstream recyclers and refineries for reuse. These refined commodities are then usually made into new products by manufacturers.

There have been occurrences, however, in which these steps have not been taken, and devices end up dumped in developing countries. When this happens, it not only becomes an environmental disaster, but leaves you at risk of data exposure and a PR nightmare

E-WASTE RECYCLING

The best media and IT asset disposition programs should go beyond the simple destruction of devices that are no longer needed. These processes should also address, and go to great lengths to mitigate, the impact on the environment.

Driven by governmental regulations and internal initiatives, organizations are sharpening their focus on managing e-waste. Many companies realize that sustainable disposal practices play an increasingly critical role in their ability to support environmental stewardship and uphold compliance obligations.

It's essential to work with an IT asset disposition partner who makes security and the environment top priorities.

Be sure to ask potential providers the following about their environmental practices:

- Will you destroy the data on our assets before recycling?
- Can you de-manufacture our e-waste into parts and properly recycle these pieces?
- Are you able to confirm that the e-waste will never be exported, incinerated, or sent to a landfill?
- Do the same security and chain-of-custody measures employed during the IT asset destruction process extend to e-waste recycling?
- Does your recycling program comply with the e-Stewards or other industry-leading standards?

CONCLUSION

Electronics recycling is often viewed from an environmental perspective as preserving resources and minimizing waste, but these services can provide much more value than that. IT asset disposal and electronics recycling should be taken seriously, and consideration is given to all aspects of its security to ensure your company's data, brand, and liability is protected.

ABOUT TELLEREX

Tellerex is committed to leveraging our knowledge and experience to reduce atm expenses, increase reliability, and accelerate a contribution to your company's bottom line. Contact us to learn how our complete ATM management solution can simplify the end-to-end process and required oversight for your ATM and cash recycler networks.