FIVE WAYS TO STRENGTHEN YOUR IT ASSET DISPOSITION (ITAD) SECURITY

WHITE PAPER

SIMS RECYCLING SOLUTIONS

It’s always in your best interest to protect data stored on IT assets, whether working or not. Without structure or guidance however, data stored within servers, hard drives, mobile devices and other IT equipment could exist even when you thought you had it all removed.

In an evolving environment IT leaders continuously need to understand new methods for data protection. Only in the last six or seven years has U.S. legislation recognized the need for secure data removal when IT assets are collected for disposal, but currently there is no existing federal law regulating the collection and usage of personal data.

Europe began taking action towards unifying data protection with the introduction of a single law, the General Data Protection Regulation (GDPR). This law was recently adopted in April 2016 and is coming into force in May 2018 and will provide structure for businesses anywhere in the world to securely collect, store and use personal information of European Union citizens.

Other parts of the world have laws regulating data privacy, hosting and protection but are either industry specific or don't cover all devices. Regardless, with advances in technology and the increase in cloud computing and connected devices, any/all regulations will need persistent updates to remain effective.

The development of these data security regulations is largely inspired by the growing awareness of existing data threats and risks. More businesses today are privy to the damage one data breach can cause. Big-named brands who've suffered a data breach have had to be the example to the industry and showcase the effects of allowing a (what may have appeared insignificant) gap in security. Compliance issues, lawsuits and reputational damages are among the most destructive and are likely to result after suffering a data breach.

> Nearly **two-thirds (64%)** of consumers are unlikely to do business again with a company that experienced a breach where financial information was stolen.

In fact according to a worldwide survey nearly two-thirds (64 percent) of consumers say they are unlikely to do business again with a company that experienced a breach where financial information was stolen. In addition almost half (49 percent) had the same opinion when it came to data breaches where personal information was stolen.

Therefore, today businesses are focusing on ramping up their cybersecurity and in knowing this; data thieves may try to search for the less-common security gaps where there may not be as much resistance. Security gaps often overlooked are those that exist during IT asset disposition. Thankfully, there are things you can do to ensure that at least during the disposition of your IT equipment, those gaps are filled.

1. Confirm data wiping is executed properly.

Various options for data wiping exist and there are programs you can purchase or companies who can do this for you. If done correctly, data wiping procedures are generally 99.999 percent effective, a percentage acceptable even for the U.S. Department of Defense, the German Federal Office for Information Security (BSI) and the UK HMG Infosec Standard No. 5.

While performing this task internally can be a convenient and more cost-effective solution, we like to point out the statistic holds true only “if done correctly”. Therefore, it’s recommended to ensure accountable data destruction by outsourcing this service, especially for companies in need of wiping a large amount of hard drives. It is advised to work with a vendor capable of maintaining the system development to support ongoing updates as well as fail-safes for scenarios where the wipe is unsuccessful. This will help you feel more confident that your vendor is continuing to improve their systems so you know their solution today, will also be viable tomorrow. Your IT asset disposition vendor should have the operational excellence to ensure nothing will slip through the process and they should also be cognizant of any updates or challenges with data erasure. Recently, for example, there have been issues with the wiping of solid state drives and some models of mobile devices.

Otherwise some vendors offer secondary verification of hard drives. This is a process where the vendor will take a percentage of your wiped hard drives and verify again that all data is removed. This could provide you further reassurance that all data has been removed securely. This type of service is generally performed on a regular basis to maintain the quality of the service and ensure data wiping accuracy. If working with a vendor, they can help you evaluate the value of the drive to determine if wiping is needed. In some cases physical destruction of the drive may be more cost effective.

Either way, if this is a task completed internally or through a vendor who solely offers data wiping, what happens to the physical hard drive? A couple of companies are able to offer holistic solutions that also provide the option to reuse or resale your equipment providing you with a higher value recovery opportunity and an environmentally responsible solution. It is advised to be very selective if you do choose this route by starting with the development of a comprehensive RFP to assist you in your vendor selection.

2. Review the security of equipment during transit.

Electronics tend to be some of the more sought after products when referring to cargo theft. In 2012 Freight Watch International provided a global average value per theft incident of $382,732 for electronics and this didn't take into consideration the value of the data stored. With a variety of solutions for data wiping the first step is getting the equipment to the facility so these services can be conducted. Internationally there is an association setting standards for secure transportation referred to as the Transported Asset Protection Association (TAPA). The certification available through TAPA is one to note however a physical examination of the transportation process is the best approach to ensuring your equipment will arrive safely.

It is important to point out that when a vendor drives away with your retired IT equipment the risk isn't removed as well. If a company's laptop was stolen from a truck and data were exposed, the company not the transportation vendor would be liable for any implications of the data exposure. Therefore it's always recommended to have a dedicated truck holding only your material with a seal on the back of the truck with the number recorded prior to departure and upon arrival at the processing facility.

Alternatively, over the past five years more on-site options for data destruction have arisen. Sims Recycling Solutions in particular has mobile shredding vehicles with shredding technology that can physically destroy thousands of hard drives per day. This service can begin with wiping and/or degaussing of hard drives right in your office. Hard drives can then be loaded onto the truck and fed through the physical shredding system right then and there.

3. Verify asset tracking and facility surveillance.

While it's important to ensure secure transportation of IT assets it doesn't just end there. The next step is making sure all items will remain secure once they arrive. Security and tracking of IT assets while they are processed at the vendor facility is important for a few different reasons. The security features of the building (which should involve restricted access, 24/7 surveillance, on-site guards, metal detectors and more) will protect any confidential or proprietary equipment that could potentially exist. Otherwise thorough tracking of assets through serial number capture, scanned barcodes and sophisticated internal reporting systems will provide you with the ability to understand where your assets are and track these items for internal records.

There are certifications that are valued in the industry which are aimed to help businesses identify and understand security measures in place. In understanding security measures more efficiently, IT executives can quickly and easily narrow down their vendor selection. Certifications to note include the following:

- **ISO/IEC 27001** is a standard that introduces best practices for organizations to manage the security of assets such as financial information, intellectual property, employee details or client data. This global certification is valued among the other ISO standards and is one becoming more common in the IT asset disposition industry.
- **The Asset Disposal and Information Security Alliance (ADISA)** is another standard based in the United Kingdom and launched in 2010, which is specific to the IT asset disposition industry. Assessments for this certification involve unannounced operational and forensic audits by United Kingdom Accreditation Service (UKAS) certified auditors. This provides global businesses with reassurance that certified vendors operate to the highest industry standards and reflect best practices for the handling and carrying of IT assets at their facilities.
- **The National Association for Information Destruction (NAID)** is the standards setting body for the information destruction industry. NAID AAA certification verifies the qualifications of certified information destruction providers through a comprehensive scheduled and unannounced audit program. This rigorous process supports the needs of organizations around the world by helping them meet numerous laws and regulations requiring protection of confidential customer information.

4. Understand resale channels and confirm ethical methods for reuse.

While data security is priority, some vendors offer solutions for the hardware disposition as well. If any equipment still holds resale value, refurbishing and remarketing services can be a great way to maximize your return-on-investment. This is an area however, where you must proceed with caution.

It is usually ideal to work with one vendor. However even if you're comfortable with one service your vendor provides it is smart to do your due diligence and understand all services offered, as if you were using separate companies for each service. In the long run it'll prove worthy of your time.

Potential risks include the following:

- Selling equipment with data that remains or is recoverable,
- Poor tracking of assets (leaving question to the inventory of remaining assets), and/or
- Pricing items inaccurately (forgoing potential returns).

There are a few things you can do to add credibility to a vendor's reuse processes.

1. Determine how items are resold

   If a company uses an ecommerce platform, such as eBay, look up and review their profile to understand their user ratings and become familiar with the inventory and buyers.

2. See the process firsthand

   If possible, go to the site and witness the operation in action. Do the employees appear to have strict standards and protocol? Are the services being conducted in a secure environment? Are items being handled carefully and are they cleaned prior to being packaged and resold?

Often knowing and understanding the infrastructure can provide a better eye for questionable processes.

5. Confirm end-of-life assets are shredded and recycled

If all data has been destroyed and an IT asset no longer holds any resale value, end-of-life disposition would be the next step. It is important to ask questions about the final disposition of your end-of-life IT assets because if done irresponsibly your company would suffer the repercussions. There are parts of the developing world illegitimate recyclers have used to dump old e-waste. If your equipment ended up in a third-world country someone could potentially pull the asset tags and determine you were a company contributing to the toxic environment and wrongful disposition of e-waste.

Whether you or your vendor is managing data wiping the process should include removal of hazardous components, shredding of equipment and then separation of the shredded commodities. Those commodities of value are then sent to downstream recyclers for reuse. Those refined commodities are then sold to manufacturers to be made into new products. Recycling vendors usually provide certificates of destruction and recycling. In some cases you can witness the destruction providing you with an additional certificate of witnessed destruction as well. These documents could be helpful for compliance or security documentation as well as for any reporting or recognition for environmental efforts. This service also leaves you with the peace of mind in knowing your old equipment is shredded into pieces, leaving minimal risk for data retrieval.

As data breaches become more sophisticated there will only be an increasing number of security protocols to watch for. As a recipient of the 2016 Computer Security Magazine's "Secure Data Erasure Company of the Year" award, Sims Recycling Solutions (SRS) recommends on-site data destruction services when possible. The on-site services provided by SRS can provide high-level security services that provide businesses with maximum return. Otherwise these five considerations should help validate your vendor selection and avoid any risks tied to data exposure as a result of IT asset disposition.

The Contract is Managed by:
Sims Recycling Solutions
info.national@SimsRecycling.com
www.simsrecycling.com