SECURIS℠
IT Asset Auditing, Recycling & Destruction

Daniel P. Mattock, Securis (www.securis.com), 9/17/14

Best Practices for IT Asset Disposal (ITAD) in a Rapidly Evolving IT Infrastructure Landscape

As Big Data, cloud migrations and mobile devices become ubiquitous in enterprise landscapes, IT infrastructure tracking and security needs continue to evolve rapidly. While procuring IT assets and managing and securing their location during use is typically a strong focus within organizations, a lack of focus occurs during the disposal of these IT assets at their end of life. The rapid evolution in IT infrastructure landscapes coupled with a lack of focus on end of life disposal has left data security holes and environmental liabilities for enterprises. This article will explore these new "blind spots" and provide instruction on the best ways to stay protected in this new IT landscape.

Properly disposing of IT assets and hardware has been a problem for enterprises and organizations for quite some time. Ever since the first computers rolled out of factory floors back in the early 1970s and started dotting the corporate landscape, IT asset managers have been tasked with finding appropriate ways to remove and dispose of the equipment. While the task has gotten easier over the years—in that a computer no longer takes up an entire office floor like the Electronic Numerical Integrator and Computer (ENIAC), an 1800 square foot computer used by the US Army Ballistics Research Laboratory in 1946—new challenges have emerged. A primary challenge is that data is everywhere. A corporation's entire list of trade secrets can fit in a pocket, and while the weight of the equipment to dispose of has gotten lighter, the data security burden associated with devices has gotten heavier.

So, how is an IT asset manager supposed to successfully navigate the complexities of proper ITAD? First the "hassle factor" associated with disposal must be overcome. It is rare that an IT procurement officer is thinking about disposal—let alone planning for it—when new equipment is purchased. The procurement officer has a whole list of other things to think about, such as the following:

>> Will the equipment help solve the business challenges for which it was purchased?

>> Is this the best value for our investment?

>> Will the equipment make our operation more efficient?

>> Is it compatible with the existing IT infrastructure?

>> Will the equipment be secure and protect data?

It is only the highly skilled and advanced IT asset manager who has the foresight to think upfront about the equipment's end-of-life disposal, not to mention the hassle of tracking it and the physical logistics of removing it from the office or facility. IT equipment can be heavy, it can take up space, and it can continue to pile up until it is a silicon and plastic landslide risk ready to topple over on the next innocent systems engineer who comes within its reach. Its disposal can also be expensive. While there are currently various free or cheap options to dispose of IT equipment, the adage that you get what you pay for still stands. If a company is taking equipment away for free, most likely they are selling it to cover their costs. The following associated questions combine to keep IT asset managers up at night:

>> Who are they selling it to?

>> Is it ending up in third-world landfills?

>> Is the disposal company complying with data security and environmental laws?

>> If not, could this equipment get traced back to our organization?

>> If so, will someone lose their job?

Given the associated hassles and costs of IT equipment disposal, managers are faced with the temptation to junk the equipment in a local landfill and call it a day. And, in the short term, some may get away with this. In the long term, however, it is a dangerous game of Russian roulette that hurts the environment and can be traced back to the company via the equipment's serial number. If there is a data breach, the company and/or the IT asset manager could be featured adversely on the cover of the New York Times.

If the trash-it approach is not utilized, there are various public programs to get rid of eWaste that may be more appropriate. The equipment can be sold, donated, or traded back to the

original equipment vendor. Keep in mind that while residual value may be earned from the equipment, selling it takes time. Those employed in IT organizations are most likely already capacity constrained and the last thing these employees need to do is spend their valuable time managing eBay auctions and Craigslist posts. Trading in equipment to original equipment vendors is an option, and some vendors will offer credit for it but it can be a burden to organize and coordinate. The data on the devices is still an issue and must be protected. Returns including original hard drives yield more residual value but doing so increases the risk of a breach. Most leading security-conscious organizations remove data storage devices and hard-drives before they return the equipment.

When letting go of retired IT assets, it is also important to consider the export issue. Where is the equipment going after it has been given to a third party? Is it being recycled correctly and properly, or is it winding up on a barge headed straight to a third world country where children break it down for scrap value? The latter scenario is not only a strain on the environment as hazardous materials can leak from the equipment, but it also can be very dangerous to an organization's reputation. No responsible corporation or organization wants to be tied to end of life equipment arriving in an unregulated third world landfill that becomes a hazard to children's health. Keep in mind as well that the data on the devices remains critical. If the data has not been properly destroyed, there is still a risk of a major data breach.

How do companies navigate the minefield of hidden traps and snares of exports and data breaches? Many companies destroy data in-house and dispose of the equipment, or outsource either the data destruction or disposal process, or some combination thereof. Either way, when using a vendor, it is important to put the vendor through the proverbial ringer to ensure that the organization's best interests are protected. A combination of detailed vendor questioning and stringent auditing is a best practice. Below, please find recommended questions to ask each eWaste vendor under consideration:

- >> What are the vendor's processes and procedures for destroying data that remains on the device? Note: The vendor should be able to provide written certification that ALL data was destroyed, as well as a record of the method used.
- >> Does the vendor follow any recognized best practices?
- >> Who certifies and audits the vendor's processes?
- >> Can the vendor produce evidence that it has proper facilities, training and equipment?
- >> What certifications does the vendor have?
- >> Has the vendor had any safety violations?
- >> Does the vendor send equipment to third party partners? If "Yes," what are their processes and procedures?
- >> Does the vendor have strong record-keeping practices (shipment records, serial tracking)?
- >> What percentage of materials is recycled vs. destroyed?

It may be beneficial to draft a score card and rate the vendors accordingly.

Audits of potential vendors should be performed on a regular basis. Unannounced, onsite audits are the most effective. There is no substitute for engaging the vendor at their location. It allows understanding of their security measures and facility as well as the opportunity to build a personal relationship with their team. However, these audits can be expensive and time consuming. If there is no budget to perform audits on a regular basis, a good alternate technique is to check the vendors' certifications. Are they up to date? Do they address your need for security and environmental responsibility?

Beyond vetting appropriate ITAD vendors, IT asset managers must also ensure they are complying with the data destruction legal and regulatory environment. The regulations can be extremely complex. However, an IT asset manager doesn't need to spend a decade earning a PhD to become an expert in the *Basel Convention on the Control of Transboundary Movements of Hazardous Wastes* and their Disposal, FACTA, Graham Leach Bliley, HIPPA, HITECH, PCI, NIST 800-88 and the multitude of other regulations. Instead, look for the following environmental and data security certifications as a shortcut to see how a vendor is complying with industry regulations.

Environmental Certifications

The two current leading eWaste certifications are R2 and e-Stewards. The R2 Standard was developed through a joint process with the EPA in 2008, and consists of a range of industry stakeholders who continue to provide feedback to advance the system. There are currently more than 530 R2-certified facilities in the world in 17 different countries. E-Stewards evolved from the Basel Action Network, a nonprofit group dedicated to ensuring the proper disposal of eWaste. There are more than 170 e-Stewards certified facilities in the world in multiple countries. It is difficult, if not impossible, to determine whether one certification is better than the other. While activists from each organization will argue until they are blue in the face about how they are different and better than the other, the reality is that each certification has significant similarities. They are both

organizations that help to motivate electronics recyclers abide by best practices in terms of ensuring hazardous materials from eWaste companies avoid landfills, that working conditions for eWaste employees are safe and that obsolete electronics aren't shipped to third world countries and recycled outside of the rules, laws and regulations of those countries. The U.S. Government recommends use of companies with either of these certifications. While in the past, some have argued that e-Stewards was the stronger certification, the R2 organization (now renamed **SERI**—**S**ustainable **E**lectronics **R**ecycling **I**nternational) is rolling out R2:2013 which will require all R2-certified companies to meet higher standards by the end of 2014. With these more stringent requirements, discerning the differences between the certifications will become even more challenging.

Data Security

On the data security and destruction side, the landscape is more complicated. This increased complexity stems from the fact that over the life of data security and information protection regulations, many government agencies got involved based on the type of data that was being stored. For example, Health and Human Services (HHS) regulates and enforces laws pertaining to protected health information (PHI) through HIPPA and HITECH. For financial data, depending on the type of institution holding the data, any of the following institutions may be involved in the enforcement of data protection: the SEC, Office of Comptroller of Currency, Federal Reserve Board, FDIC, Office of Thrift Supervision or the National Credit Union Administration. Moreover, 47 of the 50 states and the District of Columbia all have separate data breach notification laws. How can aspiring professional IT asset managers abide by the right regulations? One method is to select vendors that are certified by the National Association of Information Destruction (NAID). NAID is a third-party industry association that audits and ensures vendors are abiding by best practices in data destruction. From making sure that employees have up-to-date background checks to making sure vendor facilities have appropriate access controls and other security measures, NAID checks and ensures that vendors are abiding by the complex multitude of regulations among the various regulatory institutions. In other words, if a NAID-certified vendor is used, from the eyes of the regulators, due diligence is realized. Some vendors will boast that they are a NAID member to try to convey the same level of security and procedural sophistication as certification. There is a big difference between being a NAID member and achieving NAID certification. A vendor can become a NAID member by little more than simply paying annual dues to NAID. However, a NAID-certified company must adhere to a strict list of data security measures and is subject to unannounced audits throughout the year. Don't be afraid to ask potential vendors for proof of their valid NAID certification.

It is important to remember that regulatory compliance does not to equate data security. A new blind spot that IT asset managers must be aware of is that certain forms of traditional data destruction are becoming—and will continue to become—obsolete. Data destruction equipment that has been used in the past may no longer be an effective method of destruction. Some of the most advanced data centers and forward-thinking organizations are well on their way to transitioning their IT storage infrastructures from those that use traditional magnetic platter-based hard drives to those that use solid state hard drives (SSDs). Magnetic platter hard drives store data on the magnetized spinning platters within the device, while SSDs store data on static memory chips within the device. While magnetic drives are currently less expensive from a per megabyte of storage capacity basis, shrewd data center managers are realizing the total life cycle cost of a SSD is beginning to become competitive with those of traditional magnetic platter drives. SSDs tend to not fail as often and last longer given that they contain fewer moving parts than those found in magnetic platters. On the surface, an inattentive IT asset manager may question, "Why is this relevant to me? A hard drive is a hard drive is a hard drive." However, the reality is that different models of hard drives can be worlds apart. And the importance here is that if the movement towards SSDs prevails, a whole industry of data destruction equipment could become obsolete. Historically, a degausser was used to destroy hard drives. A degausser is a data destruction device containing magnets that, when run over the magnetic platters of traditional magnetic platter hard drives, scrambles the data making it unrecoverable. The best degausser on the market is harmless against a SSD. There are no magnetic pieces within a SSD, so using a degausser is ineffective. That leaves two optimal methods to destroy data on solid state drives. The first is with wiping software. While there are various wiping products on the market, destroying data in this way can be costly and time consuming. Wiping products simply write new data over existing data, so, the larger the storage capacity on the SSD, the longer the wait for the drive to be overwritten. IT managers, like most employees, are already busy. Top managers are looking for alternate approaches. One of the best approaches is to physically destroy these drives using a microshredding device. Vendors with these devices can bring the shredder onsite to perform the work. The process is fast (often no more than 5 seconds per drive) and environmentally friendly if the vendor has a strict recycling policy. How small should material

be shredded? Given that the chips that store data can be as tiny as ½" by ½", the NSA currently recommends that material be destroyed to a 2mm particle size. (Source: NSA/CSS Storage Device Declassification Manual) Starting to plan a strategy now for the future destruction of SSDs in advance of this upcoming infrastructure shift is prudent and valuable to your organization.

We've taken a look at some of the best ways to manage ITAD and some of the ways to protect against blind-spots in the new IT infrastructure landscape. What does the future of ITAD hold and what innovations can we expect to see in the next several years? From a technology perspective, more and more software will be integrated into the process, both when it comes to erasing data on hard drives and to track, monitor and manage ITAD. Software will advance to help managers control both compliance and security. This software will come in the form of user-friendly, cloud-based online inventory portals and mobile apps. We also expect to see advancements in tracking and scanning technologies. These innovations in tracking automation will help IT asset managers save time and result in more accurate and secure inventory records to facilitate audits and security. Lastly, we expect to see an increase in GPS usage in tracking assets. While GPS monitoring already takes place on the front end of IT asset procurement, we expect to see this more and more on the disposal side; especially in transporting assets that contain data. These are exciting times to be in the field of IT asset management, and by embracing these upcoming advancements, IT asset managers can continue to successfully lead their organizations' IT asset strategies for years to come.

About Daniel Mattock

Mr. Mattock has over fifteen years of experience as a business executive and IT risk management specialist. His experience includes private equity investing, technology and government M&A advisory work and environmental building and real estate development. In 2011 Mr. Mattock joined Securis, a leading IT Asset Disposal and data security company servicing government agencies and enterprise customers. He currently serves as its Executive Vice President where he helps develop and execute secure IT asset disposal strategies for its diverse, global customer base.

Mr. Mattock is a LEED Green Associate as certified by the U.S. Green Building Council and a Certified Secure Destruction Specialist as certified by the National Association of Information Destruction.

Away from the office, Daniel enjoys spending time with his wife, daughter, family, and friends. He also is active in his church and with the Juvenile Diabetes Research Foundation.

About Securis

Securis is an industry-leading provider of information technology asset disposal (ITAD), including ultra-secure recycling, auditing and destruction services for PCs, hard drives, servers, smart phones and other electronics.

Securis is approved by the U.S. General Services Administration (GSA), certified by the U.S. Defense Logistics Agency (DLA) Logistics information Service and is one of a handful of companies to hold certifications from both R2 and the National Association for Information Destruction (NAID). Securis is 100% compliant with all U.S. federal, state, and local data security and environmental regulations.
For more, visit www.securis.com.

1.800.731.1909 | securis.com