Safety First Data Disposal Practices

By Michael Harstrick
Chief Global Development Officer

As companies enter the next phase of the battle against COVID-19, the safety of employees and the security of their facilities remains a key concern. That includes how decommissioned media and sensitive data is eliminated.

Is your IT closet stuffed with old disk drives and tapes that need to be destroyed? You are not alone.

In light of the ongoing Shelter in Place (SIP) restrictions, a key consideration is whether to go with in-house, onsite disposal or outsourcing.

Outsourcing your data disposal needs has its benefits. You make a phone call and the company arrives with its team of professionals and sanitizes or removes your unwanted hard drives and tapes. Out-of-sight. Out-of-mind.

Yet in today's environment, outside vendors coming into your facility may present unknown risks. Companies that have started to reengage workers are requiring a range of safety measures.

These include "regular health screenings at entrances and requiring workers to wear face masks and other protective gear on the job. Many companies are changing floor plans, rerouting workers through separate entrances and exits, and staggering shifts to limit interaction," according to the Wall Street Journal.

These measures impact both your employees and your outside vendors.

The better alternative is to contain your data disposal in-house with your own equipment, operated by your in-house team on your schedule.

With in-house data disposal your company gains:

- The ability to immediately erase the data without stockpiling.
- Absolute control over the entire data elimination process.
- Assurance that all compliance regulations are followed, chain-of-custody is maintained, and physical data breaches are prevented.
- Accurate tracking and documentation to withstand the scrutiny of data security audits.

Choosing the right approach

You have many options when it comes to choosing in-house data elimination and destruction methods.

Overwriting. This may appear to be the easiest approach but actually takes the most knowledge to ensure compatibility of equipment. Overwriting is a time and energy intensive option, generally taking 8 to 14 hours for each drive. But be careful. Overwriting is not an NSA or DoD approved form of sanitization. Also, it can only be performed on fully functioning hard drives. Overwriting is the lowest level of data security for your organization.

Shredders. Shredders physically destroy your drives. However, physical destruction is not enough as I shared in a previous LinkedIn article. Recovering data from destroyed hard drives is easier than you might think: even when that disk drive fell from the space shuttle, burned on reentry and sat in the dirt for six months.

Degaussers. Degaussing — removal of all data from hard drives and tape media through demagnetizing – provides the most secure method of data elimination recognized by the NSA. Degaussing takes less than one second to completely eliminate all data on any size hard drive. When you degauss your drive, regardless of whether

you physically destroy it, you have performed the most secure method of data destruction. Degaussing provides complete protection for your organization.

Destroyers. High-quality hard drive destroyers bend break and mangle hard drives and internal components — including the data platters, PC boards and read-write heads. Hard drive destroyers physically damage the media which makes data recovery more challenging. They provide visual verification that the media has gone through a data destruction process prior to media disposal. Because destroyers alone lack the data elimination aspect that degaussers perform, it is best practice to destroy drives after degaussing,

For fully secure data elimination and destruction, degauss *and* destroy your hard drives and tapes.

Purchase considerations

When choosing your data elimination equipment, consider the following:

- Level of security needed. Your vendor should offer a range of products -- from those designed for quiet office operations to NSA-listed equipment developed for the elimination of TOP-SECRET data.
- Ease of use. The equipment should be easy to use by non-technical staff through a simple one or two step process.
- Transportable. For the most convenient data elimination, choose equipment that allows you to destroy data at the removal point. A rolling, easily transportable, high-quality cart allows you to degauss and/or destroy data as it is removed from the rack.
- Verification. Be sure your equipment allows you to accurately verify, document and preserve your process in a traceable log and generate a certificate for proof of erasure and destruction; including serial numbers and images of the media.

Garner products offers a full line of degaussers and destroyers complete with our IRONCLAD audit verification system. To learn more, visit GarnerProducts.com.