Words: 800

Questions to Ask Your Vendor about Data Destruction

Every day the media publishes stories about companies whose data resources are hacked, with loss or theft of private corporate and personal data. Whereas many of these incidents involve people using active computer devices with all sorts of security software and processes in place, they also involve organizations and municipalities whose hardware assets were retired but not properly disposed.

How is this possible today when companies are buying data destruction services that should be successfully removing/destroying data on those obsolete storage devices? The key is asking your vendor the right questions.

Get Informed - Ask Questions

Today, numerous websites and vendors sell “data erasure services”. These promise to eradicate data from the associated hardware. Other terms for this service are data clearing, data wiping, and data destruction. This solution is often a software-based method that overwrites the data with 1s and 0s with the purpose of destroying all electronic data residing on the digital media. But is this method 100% effective? And can you rely on a technician at your company manually performing this task as the volume of end-of-life devices increases?

The vendor who is selling you services to dispose of your IT assets must not only understand your data destruction requirements but also be an expert in the solution technologies to achieve those objectives. Ask your vendor about its certifications. IT Asset Disposition (ITAD) experts are supposed to have the knowledge and experience in industry standards and best practices for IT lifecycle management. This involves continually updating their processes and certifications for limiting customer data liability. Your vendor should be capable of explaining the pros and cons of the different destruction options for disposing of your hardware and the associated costs.

Here are a few key questions you should ask your vendor about data erasure solutions.

Q: Why should I be cautious of low-cost erasure solutions?

A: Low-cost, unlimited solutions often do not include certifications that meet strict standards. As a result, they often have high failure rates on systems they process. Ideally, the erasure process should:

- Allow for selection of a specific standard, based on your unique needs
- Support erasure of the type and number of devices being erased, and
- Provide verification that the overwriting method has been successful and removed data across the entire device.

Q: Does the solution meet my compliance needs?

A: Verify that the vendor’s recommended solution meets your specific compliance requirements (e.g., Sarbanes-Oxley, PCI, HIPAA, HiTECH, NIST standards) and provides the related audit trails and reports you will need to retain or submit to regulatory authorities.

Words: 800

Q: Does the solution help us save costs by improving our process?

A: The best solution should provide cost-effective performance that meets your business data risk and compliance objectives and your device end-of-life goals. This requires both business and technical acumen from your advisor. It also requires process automation that removes the manual reporting and processing.

Q: How long should a disk wipe take to complete?

A: A comprehensive erasure tool should securely overwrite any device at 30-40 GB per minute. New flash media and encryption removal technology can make this process even faster. Be aware that low-cost tools may lack the appropriate drivers and ATA commands to efficiently erase your device.

Q: How many times should an ITAD wipe a computer?

A: According to Bernard Le Gargean is the Product Manager of Blancco Drive Eraser, "One pass is enough. However, to ensure the overwriting process has been effective, major agencies and government bodies worldwide (NIST 800-88, NCSC, BSI and others) state that the verification of data erasure is mandatory for full compliance with their standards. Other research supports this idea."

Q: How should I verify erasures?

A: Your vendor and solution should consistently check drive wipe results to verify that data erasure tools are functioning properly.

A: How long should I store audit reports?

Q: Store audit reports a minimum of 7 years or as required by your policy advisors or government regulators.

Work with a Trusted and Experienced Advisor

Castaway Technologies believes you should be as informed as possible about the latest best practices for safely and securely mitigating risks involved with the turnover of data-bearing IT assets. This will allow you to focus on what really matters – running your business.

While most companies focus on the initial phases of the IT lifecycle, Castaway is the premier ITAD specialist that works with businesses and organizations to streamline the end of their IT lifecycle processes. Recently, Castaway was granted AAA Certification by NAID® (National Association for Information Destruction), a division of the International Secure Information Governance and Management Association™ (i-SIGMA™). These organizations set the standards for best practices in the ITAD (IT Asset Disposition) industry.

For further information about your data destruction needs, give us a call.