
# Is Data Encryption Enough When Retiring Hard Drives?

# Introduction

Encrypting hard drives adds an effective new level of data protection and security for organizations. However, there is a disturbing trend of relying upon encryption as the sole form of data sanitization. While encrypted data may seem inaccessible it should never be considered 'sanitized' because the data is still there. As long as the data remains on the drive, encrypted or not, it is subject to a number of risk factors.

To ensure maximum security, data should still be erased or destroyed in a secure and permanent manner. IT managers can use encryption technologies hand-in-hand with data erasure tools to provide an optimized and secure process for handling decommissioned computers and hard drives.

## Software Encryption vs. Self Encrypting Drives (SEDs)

This article addresses both software encryption methods as well as Self-Encrypting Drives (SEDs). In general using SEDs is superior to software encryption because it currently has fewer known attack vectors. Many of the concepts addressed here apply to either method of drive encryption.

## Encryption is not a proper sanitization method

### RISK: The data is still there

Relying solely upon encryption to protect data on a retired hard drive exposes organizations to inherent risk because the data remains on the drive. Future potential risks, such as changes in encryption or decryption technology, may compromise encrypted data and are impossible to predict. The fact is, if the data is still there, it can be compromised.

## RISK: Encryption algorithm weaknesses

Relying solely on encryption for data sanitization may expose you to weaknesses in the encryption algorithms themselves. Recently the New York Times reported that an algorithm for generating random numbers, which was adopted in 2006 by the National Institute of Standards and Technology (NIST), contains a backdoor for the NSA. As this example shows, it is impossible to know what future risks you might face in relation to today's encryption technologies.

## RISK: Decryption technology developments

Proponents of relying on encryption as a sanitization method argue that the 128 or 256 bit encryption used could take many years to break given today's computing power, making it adequately secure. However these calculations don't account for the advancement of decryption technologies and techniques. Developments may occur that could make today's most secure encryption technologies easier and faster to break. In fact, the federal government currently has a program to decode encrypted messages with a $11 billion yearly budget and 35,000 employees.

To illustrate this risk, here's one example of how encryption keys may potentially be broken at a faster rate. Let's assume XYZ Corp uses key deletion as their sole data-protection measure for retired hard drives. This method simply removes the encryption key on a hard drive rendering the data unreadable. The data from the drive is still there, just in an encrypted format. Now let's assume that XYZ Corp installs Windows 7 on all their machines. By comparing unencrypted Windows 7 install data with the encrypted Windows 7 install data it could give a hacker a shortcut to breaking the encryption key.

You CANNOT ASSUME that today's encryption-breaking technologies and techniques will remain stagnant. Similarly you should not leave encrypted data on retired hard drives because it exposes them to potential future risk.

## RISK: Password weakness

Some companies may decide to not take any sanitization actions based on the fact that the drive is encrypted and protected by a password. This is an extremely dangerous security practice! Passwords are notorious for being a weak form of security and are easily guessed at or broken. Tools like multi-factor authentication can make password security more effective and robust but should still never be relied upon as a reason not to sanitize a retired drive.

## RISK: Cold boot and similar attack vectors

Cold boot attacks attempt to access encrypted data by retrieving the encryption key directly from RAM. Most would assume this data can only be recovered when the computer is on, but cooling methods can be used to elongate the period of time in which RAM data stays intact. While this vulnerability exists primarily for software encryption tools and doesn't affect disk sanitization, it underscores the types of attacks that can exploit weaknesses with encryption.

SEDs are still relatively new and may be prone to similar hardware hacks. While SEDs utilize as few external computing resources as possible, such as the primarily operating system, they nevertheless contain their own hardware components such as flash memory that may be found to have vulnerabilities.

## RISK: Reporting and Human Error

One of the most important aspects of a solid data-sanitization practice is the ability to keep a secure and accurate record of all your activities. Having proof that your data was properly sanitized can provide legal and regulatory protection and makes your process easy to audit.

Current SED solutions don't provide the robust, secure reporting capabilities sufficient for sanitization tracking. Logs or reports should be verified and stored in a protected corporate location or database allowing access to key IT, regulatory, and legal stakeholders.

Without automated reporting, human error becomes a major risk to consistently and properly sanitizing hard drives. Without reporting, it is impossible to be sure that every drive was handled and verified as being sanitized.

# Redundancy is the best practice

One key best practice for data sanitization is redundancy. This may come in many forms including multiple methods of data erasure or destruction, multiple levels of data security such as encryption, or multiple reviews of processes to ensure compliance. This belt and suspenders approach to data security gives you a very high level of confidence that your data cannot be compromised.

With that in mind, simply relying on encryption to protect your data or deleting an encryption key on an SED is insufficient to provide complete protection. If the data is still there, even in

encrypted form, it remains vulnerable. In contrast, securely and permanently erasing data gives you absolute assurance there is no risk of recovery. Remove the data, remove the risk.

Here's one example of how this two-pronged approach could help streamline your hard drive retirement process. One of the security risks companies face is a long period of time between when a computer is decommissioned and when it's hard drive is sanitized. To shorten this period, you could have an IT admin delete the encryption key immediately upon decommissioning the machine. This would put the data in a much more secure holding state until it's able to be fully erased at a later time or during a batch process. Even though the encryption key deletion and data sanitization may happen at separate times, you would have a record of all actions taken to properly sanitize the drive.

# White Canyon's view on encryption

WhiteCanyon is enthusiastic about the added layer of security encrypted hard drives can provide. However, as outlined in this article, we DO NOT recommend using encryption as the sole method of data protection when a hard drive is retired or recycled. The best practice is still secure data erasure or destruction.