

# SECURING THE FUTURE

## In this Issue

- It's under lock and key so it's secure, right?
- This would never happen to our company!
- Why put your company at risk?
- What types of electronic media can be destroyed?
- Shred-it's hard drive destruction services
- Your free security consultation

Why stockpiling hard drives can be harmful to your business — the need for proper electronic media destruction protocols

*In this issue, we will discuss how stockpiling your old hard drives makes your organization more vulnerable. This begs the question: why take the risk?*

Many U.S. businesses, both large and small, may not realize that the most effective way to properly dispose of hard drives and electronic media is to destroy them. The issue is new enough that many companies' safety protocols and procedures don't account for unused hard drives and electronic media. Instead, businesses often store items with confidential information on them in a storage closet under lock and key. Despite both the short and long-term negative consequences, many U.S. businesses appear to follow this process because they are unaware of the risks to themselves and their customers.

800.697.4733 | [shredit.com](http://shredit.com)



Making sure  
it's secure.™

# SECURING THE FUTURE

## It's under lock and key so it's secure, right?

As technology evolves, misconceptions have emerged about hard drive and electronic media security. For example, locking up old hard drives in an IT closet or an off-site storage facility is often perceived as a safe option, despite being a target for data thieves. Even if organizations use software to erase, wipe, reformat and degauss electronic devices, it may not fully protect you — confidential data from obsolete hard drives can still end up in the wrong hands. Carelessness is just as dangerous, with improper destruction potentially leading to a costly breach that could damage your company's reputation. This begs the question, why risk it?

Shred-it's Information Security Tracker survey, which assessed the opinions of small and large U.S. businesses, demonstrated that 53 percent of U.S. businesses mistakenly thought that erasing, wiping or degaussing their devices before recycling them was enough to protect their confidential information from being lost or stolen.<sup>1</sup> Another 17 percent of U.S. businesses indicated that they simply recycled their old electronic media. Further, 12 percent said they didn't know how their business was disposing of its aging or obsolete computers, or other data-storing devices such as smartphones or photocopiers. Given the importance of destroying a hard drive, it's startling to think that only 1/4 of businesses across the U.S. have never used this method of destruction.



1/3 of businesses say loss of  
info would harm credibility.<sup>1</sup>

800.697.4733 | [shredit.com](http://shredit.com)

## But we are secure — this would never happen to our company!

Could it though? Recently, there was a massive laptop breach that grabbed national attention when an unencrypted laptop was stolen from the car of an employee of Cancer Care. The laptop contained the names, social insurance numbers, birth dates, diagnoses and treatment information of 55,000 current and former patients.<sup>2</sup> It was subsequently discovered that they had never conducted a company-wide risk analysis before the breach occurred.

You might be quick to point out that this is not your business and you may think that it wouldn't happen to you. You may follow policies and procedures, but do all of your employees do the same? While Cancer Care recently reached a settlement and those affected are receiving information about protecting themselves, the information breach has once again raised red flags around workplace policies and procedures.<sup>2</sup>

Below is a list of best practices to implement in your workplace to avoid data theft, including:

- Consider performing regular clean-outs of storage facilities and avoid stockpiling unused hard drives
- Destroy all unused hard drives using a third-party provider who has a secure chain of custody to help give you peace of mind and ensure your data is being kept out of the hands of fraudsters
- Consider conducting regular reviews of your organization's information security policy to incorporate new and emerging forms of electronic media



Making sure  
it's secure.™

# SECURING THE FUTURE

## Why put your company at risk?

The cost to destroy hard drives is minimal when compared to the potential risks faced when you don't. Shred-it, the world leader in document destruction, can permanently destroy confidential information at a low cost that will fit your budget. Not only that, hard drive destruction is the most effective way to permanently destroy all information. Shred-it's secure chain of custody ensures pick-up and destruction of the unit within two business days, with a Certificate of Destruction issued for your files. At the end of the day, Shred-it's Hard Drive Destruction Service will offer more than just a certificate; it offers the peace of mind you deserve as a member of the American business community.

Shred-it's Hard Drive Destruction Service fully destroys hard drives, memory sticks and photocopier memories, rendering them completely useless and beyond repair. This offering also allows businesses and IT professionals to track their information destruction history by issuing a Certificate of Destruction that lists all electronic media that has been destroyed along with individual serial numbers.

## What types of electronic media can be destroyed?

- Hard Drive (any kind of laptop, desktop, PATA, SATA and many more)
- Backup Magnetic Tapes (any kind of DLT, mini cartridges and many more)
- Floppy Disk (3.5 inch disks, 5.25 inch disks and many more)
- Zip Disk (100 MB, 250 MB and other large disks)
- Optical Media (CDs, DVDs, Blue Ray and HD DVDs)



800.697.4733 | [shredit.com](http://shredit.com)



Making sure  
it's secure.™

# SECURING THE FUTURE

## Why should you consider Shred-it's Hard Drive Destruction Services?

✓ 100% DESTROYED	Only by destroying your hard drives will they be useless to identity thieves
✓ 100% SECURE	Shred-it's chain of custody process provides end-to-end security
✓ 100% ASSURED	Shred-it will provide an itemized Certificate of Destruction for you to keep for your files
✓ 100% PEACE OF MIND	Shred-it offers a risk-free alternative to stockpiling, erasing, reformatting or degaussing obsolete or unused electronic media
✓ 100% SHRED-IT	25 years of proven and total commitment to secure information destruction

## Your FREE Security Consultation

Learn more about Shred-it's Hard Drive Destruction Services. Visit us at:  
[shredit.com/secure-hard-drive-destruction-service](http://shredit.com/secure-hard-drive-destruction-service)

You can also visit Shred-it on [Facebook](#) and [LinkedIn](#) or you can follow us on [Twitter](#) at @Shredit

- 
1. Ipsos Reid, Shred-it, 2015 Shred-it Security Tracker
  2. Lexology, 2015, Don't Lose your laptop! New HIPAA settlement emphasizes importance of risk analysis and device and media controls

800.697.4733 | [shredit.com](http://shredit.com)



Making sure  
it's secure.™