Blank is secure

Learn why it's critical to ensure that blank is done right, ensuring that data is gone for good.

Blancco IT staff in the U.S., Germany, Finland and the U.K. hit a large online marketplace to purchase over 150 used SSDs and HDDs. These were analyzed by our partners at Ontrack using proprietary data recovery tools to see if any sensitive data remained.

See what data they discovered.

There's an undeniable fascination with buying new electronics.

But tightened budgets and steeper device prices can put a damper on this desire, leaving many individuals and organizations to invest in used IT equipment and storage sold on online marketplaces.

Blank is secure, but the truth is, many of these assets have not been completely purged of the data that resides on them.

Depending on the data disposal method you've chosen, that HDD (for example) you thought was wiped clean and ready to sell for a profit may be filled with a customer or colleague's personally identifiable information (PII). Proprietary or business-sensitive documents could also be involved.

This could pose a major problem if the issue is discovered by the U.K.'s Information Commissioner's Office (ICO) or other governing bodies that may find you in breach of regulations such as GDPR.

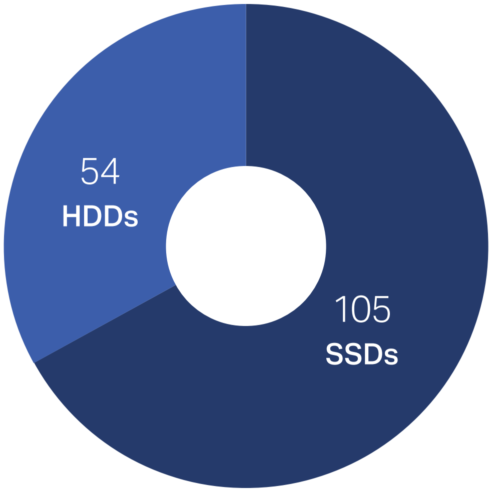
What precautions are online marketplace sellers taking with personal data when they post their devices for sale, and how likely is it for the new owner to find residual data on the device?

We conducted a study to find out. More importantly, we outlined how you can recoup costs from your used devices and drives with complete confidence.

Methodology

Between September and October 2018, Blancco IT staff in the U.S., Germany, Finland and the U.K. hit a large online marketplace to purchase over 150 used SSDs and HDDs. These drives were then analyzed in early 2019 by our partners at Ontrack using proprietary data recovery tools to see if any data, particularly personally identifiable information, remained. Drives were sent to Ontrack locations in France, Germany, Poland, the U.K. and the U.S. for this analysis. Once the recovery exercises were complete, the drives still containing recoverable data were re-wiped using Blancco software to ensure complete sanitization, and all the results were collected by Ontrack. During the process, the method of data disposal was noted, along with a description of any data recovered.

Which Storage Mediums Were Analyzed in This Study?



Study at a Glance
Total Drives Evaluated: 159
Total Drives with Some Type of Data Found: 66
Total Drives with PII Found: 25

All drives were purchased randomly, with no manufacturer or seller in mind. Therefore, a wide range of drive brands are included in the study (including Samsung, Seagate, Hitachi, OEM drives for HP and Dell and many others). Drives were also allowed to be purchased in lots, meaning several drives could be sold from the same seller or organization. The only strict requirement for purchase was that the drives had not been wiped using Blancco software.

Please note that for the purposes of this study, we defined PII as information that relates to an identifiable person. Examples include: name and other names used; Social Security number (full and truncated), driver license and other government identification numbers; citizenship, legal status, gender, race/ethnicity; birth date, place of birth; home and personal cell telephone numbers.

Results of the Analysis

Out of the 159 drives analyzed, some type of data was found on 66 of them, with 25 of the drives containing PII such as photos, birth certificates, names, email addresses and more. This means more than 15 percent of the drives tested contained sensitive information that could be dangerous in the hands of identity thieves or hackers. In other words, for every 20 drives, at least three had PII. On the other drives containing data (but no PII), system files were often left behind.

More than 15 percent of drives tested contained sensitive information that could be dangerous in the hands of identity thieves or hackers.

What did this information look like? Here are a few examples, each from a different drive or group of drives.

- References to major London universities. Some documents were found with the student names and coursework. Several student email addresses were also discovered.
- A drive from a software developer with a high level of government security clearance (DV) had family birth certificates, scanned copies of family passports, CVs and financial records.
- Office files with employee names in the metadata.
- A group of drives used in hospital equipment to record operations. No patient data was found, but a video of someone testing the camera was. They recorded out of their office window which allowed the experts at Ontrack to pinpoint the exact office in France they worked in, along with several of the car registrations from their company car park.
- Over 5GB of archived internal office email from a large travel company.
- Over 3GB of email from a cargo/freight company, along with documents detailing shipping details, schedules and truck registrations.
- Data from a school: many pictures from kids' activities, Microsoft Word and Microsoft Excel files with pupils' names and grades.
- Photos and Excel files from a religious group.
- Company information from a music store, along with 32,000 photos.
- Several drives with family photos and personal documents.
- One hundred forty Microsoft Word and Excel files, plus photos, from a school laboratory.
- Thousands of photos from a woman from Denmark, along with her name and her friends' names.

Leftover emails, photos and files can cause personal, financial and reputational damage to individuals and their employers.

Data Disposal Methods

Every seller we purchased drives from insisted that proper data sanitization methods had been performed so that no data was left behind. This demonstrates that sellers are attempting to permanently wipe data (and see the importance of this process). However, many are failing to use a fully effective solution. For most devices analyzed, formatting the drive was the data disposal method of choice. However, as the results show, this method is not always enough for complete and permanent data removal.

What is Formatting?

Formatting can go by many names, such as low-level format, deep format or full format.

In modern operating systems, there are typically two options for formatting: a full format and a quick format. Quick format is not an erasure solution because it only removes the index, but a full format attempts to overwrite the disk space visible to the OS with zeroes.

If everything goes perfectly, then one round of overwriting with zeroes will remove data. However, the key issue with formatting is that there is no way to confirm that the data is gone. Verification and certification are key to ensuring data is permanently erased beyond recovery.

Quick format and reformatting are often the default tactics for wiping data from used drives.

What's the Problem, and How Do You Solve It for Your Business?

Email, company presentations, sensitive healthcare documents, confidential company documents, photos, videos—these are all created, saved and shared across the digital universe. You may be thinking, so what? Only 15 percent of the drives we studied contained personal information. But any PII unknowingly disclosed is dangerous for individuals and businesses. Think about what an identify thief could do with the data left behind by the software developer with security credentials. Not only would a nefarious character have a goldmine with this man's information, but also with his family's personal data.

Though the software engineer should probably have known better, the challenge is that most people don't have the technical expertise of information security gurus or data recovery specialists. They do not have the necessary knowledge, skills or training to fully understand which data disposal methods are capable of erasing data forever—and which methods are not. They also have no way of verifying that all of their data was indeed removed.

For businesses, this level of residual data can be costly. Consider the potential of having 15 out of 100 decommissioned and resold servers leaving your campus with corporate data remaining. Or three out of every 20 drives sent for recycling with traces of business information. It's not unlikely. Recently, Business Insider Australia reported that Western companies often abandon sensitive, confidential, personally identifiable information to foreign companies when transitioning to new hardware.

The best method for securely erasing drives is a software-based random overwrite method. Individuals and organizations alike would be wise to understand the effectiveness of the varying data deletion/wiping methods and leverage solutions that protect the privacy of their families, customers and employees, as well as their business reputation.

What to Do Before Selling Your Drive

☑ Research the value of your drive.

☑ Back up any important data to another drive or device.

☑ Securely erase your drive by using data erasure software.

- Confirm that the software can perform the right erasure method for your type of drive.
- Confirm the total number of overwriting passes that are performed and verified by the erasure software. Each pass signifies a complete overwrite of the drive with all 0s, all 1s, or random data.
- Confirm the data is erased with an auditable, tamper-proof certificate.

☑ Double check that all your data was, in fact, erased. If you need proof that the data sanitization method you've chosen is effective, there are data recovery solutions available.

Maximize your IT investment

When Blancco's random overwrite method, including our patented SSD erasure method, was performed by Ontrack, it was 100 percent effective in every case and resulted in zero recoverable data remaining on the drives.

Even with more than 270 million erasures on the books, no data has ever been breached from a Blancco-erased device.

Blank is indeed secure.

Not only is this critical to avoid data spillage outside the bounds of your protection, but it's critical to staying in good graces with your stakeholders and government and industry regulators.

Seek security first

Data erasure is your best and final line of defense when you or a reseller markets your previously used IT assets. Find out how scalable and thorough it is.

Start your journey to blank now.

Visit our content hub