blancco
technology group

The Leftovers: A Data Recovery Study

June 2016

TABLE OF CONTENTS

INTRODUCTION

The amount of digital information stored on computers/laptops these days is staggering. It's everything from payment data used to buy products from an online retailer, personal photos and videos to confidential payroll records and classified government documents.

According to IDC, worldwide PC shipments totaled 61.9 million in the first quarter of 2016. As industry analysts explain, this decline can be attributed to several factors. One of these factors, in particular, is that users are delaying purchasing new computers/laptops due to shrinking consumer budgets and corporate IT spend. As a result, users are purchasing new drives far less frequently. On top of that, users may be in search of an extra drive to add storage to their existing computers/laptops or they may be looking to replace an old, non-working drive without spending a significant amount of money. These combined factors have driven an increase in sales of used drives in retail stores and ecommerce sites.

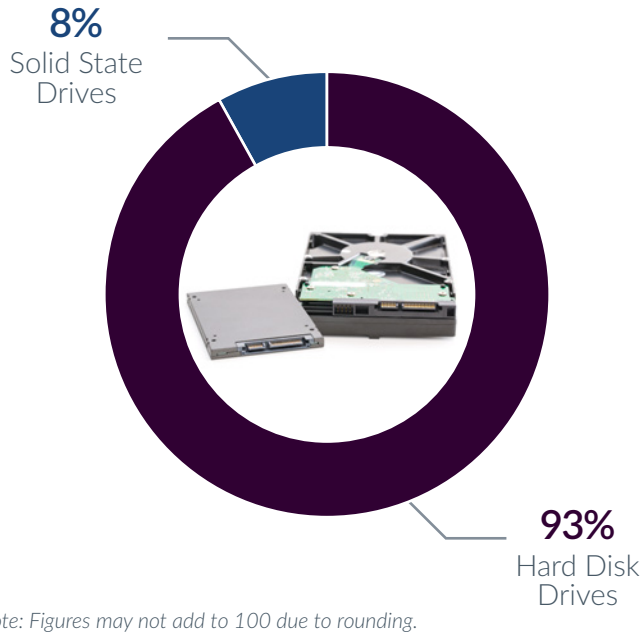
61.9 million

Worldwide PC shipments totaled 61.9 million in the first quarter of 2016.

STUDY METHODOLOGY & OBJECTIVES

Blancco Technology Group conducted a data recovery study to determine if residual personal and corporate data could be recovered from used electronics. In the first quarter of 2016, our team purchased a total of 200 used hard disk drives and solid state drives sold in the United States from the following online marketplaces: eBay and Craigslist. All second-hand drives were randomly selected and purchased based on availability.

Which types of electronics were purchased and analyzed in the study?

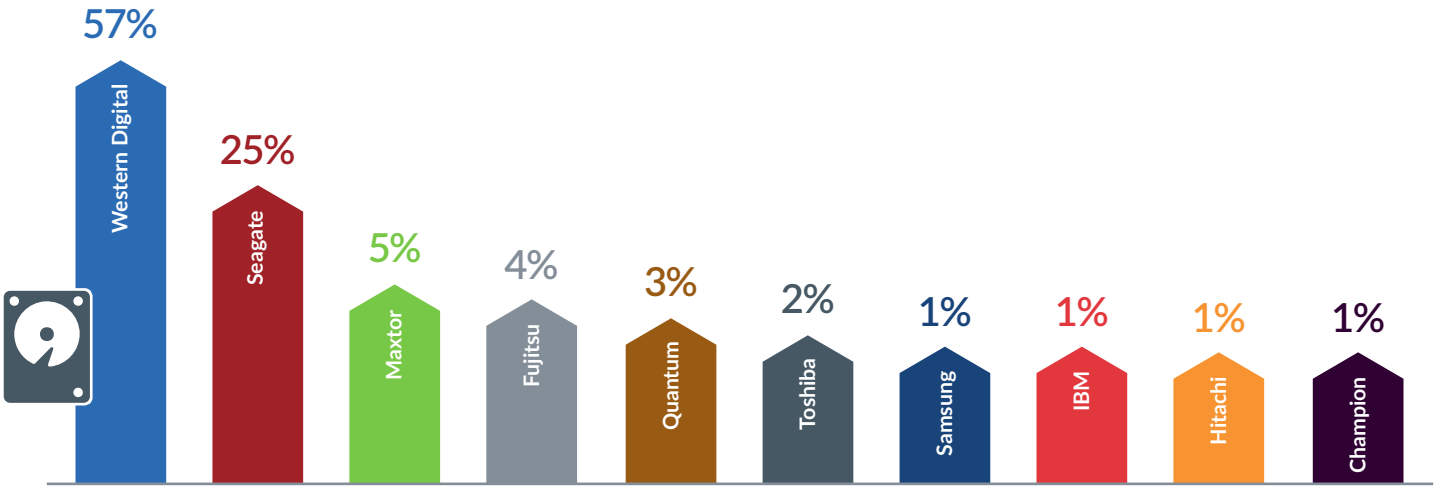


Note: Figures may not add to 100 due to rounding.

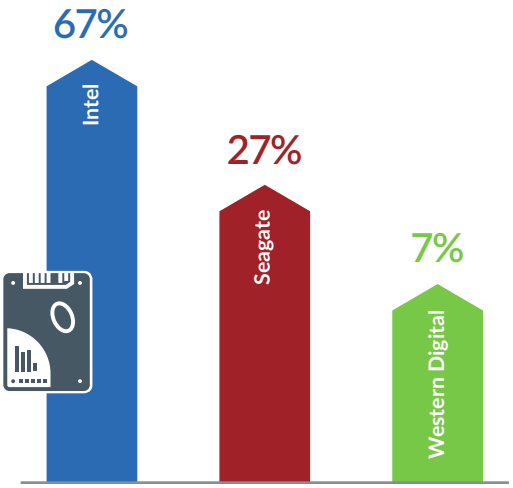
blancco technology group

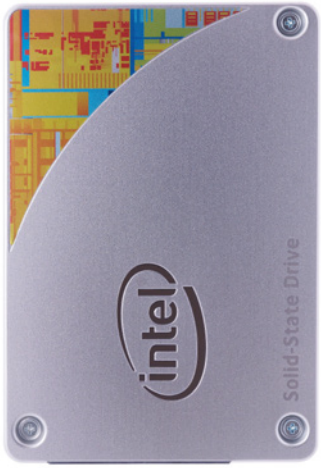
STUDY METHODOLOGY & OBJECTIVES

Which manufacturers were included in the sample of used hard disk drives analyzed for this study?



Which manufacturers were included in the sample of used solid state drives analyzed for this study?





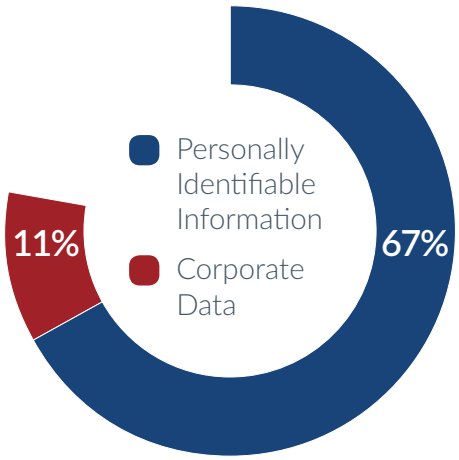
Note: Figures may not add to 100 due to rounding.

KEY TRENDS & INSIGHTS

Personal and Corporate Data Linger on Used Drives Sold on eBay and Craigslist

Out of the 200 used hard disk drives and solid state drives purchased from eBay and Craigslist, our digital forensics experts were able to recover residual data from over three-fourths (78 percent) of the drives. This finding on its own is worrisome, but when you consider that the leftover data includes both corporate data and personally identifiable information, it is clear that certain areas of data security, such as data removal, aren't given as much weight or priority as others like encryption may be.

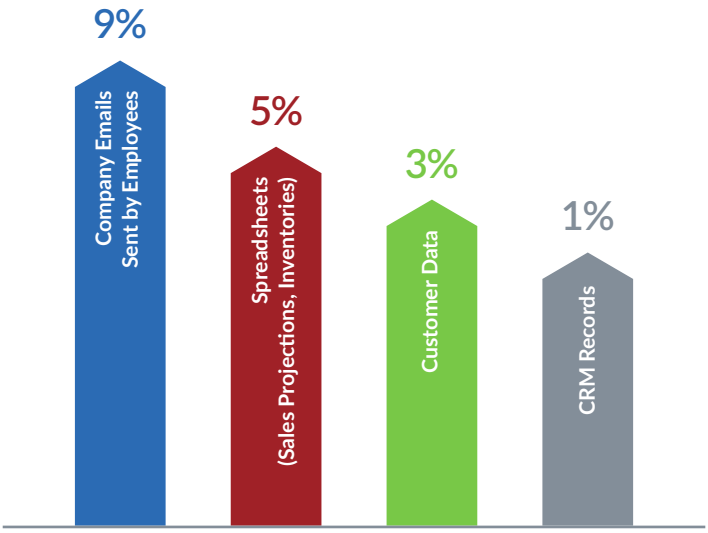
Which types of data were recovered on the used drives?



Company Emails, CRM Records & Spreadsheets Are Highly Susceptible to Leaks

Our team discovered various types and amounts of company data still remaining on 11 percent of the used drives purchased online. Upon looking closely at the specific types of corporate data accessible, company emails were found on 9 percent of the drives, followed by spreadsheets containing sensitive company information including sales projections and product inventories (5 percent) and CRM records (1 percent).

Which types of company data were recovered from the used drives?



While these figures may not seem exceptionally high, they are still alarming for several reasons. If the original owners of the drives were employed by large enterprise businesses with thousands of employees, customers and partners, it's highly likely the subjects and topics of those company emails could be extremely sensitive and potentially damaging to the employers if leaked. Given the CRM records included sales projections and product inventories, the loss or theft of such data could pose a serious threat to a company's intellectual property and diminish its competitive advantage in the market.

While some businesses may not feel erasing data is the most important security measure to take, we would caution them to look at what happened to Sony Pictures in 2014 when sensitive company information was leaked, including the salaries of top studio executives, marketing presentations, film budget data and company emails. Despite the tremendous amount of negative exposure and damages companies like Sony Pictures have endured, many businesses are still not providing their employees with the necessary tools to permanently erase their data. And in failing to do so, that puts not only their employees' personal privacy at risk, but also increases the likelihood that confidential company information and intellectual property could be at risk of being accessed.

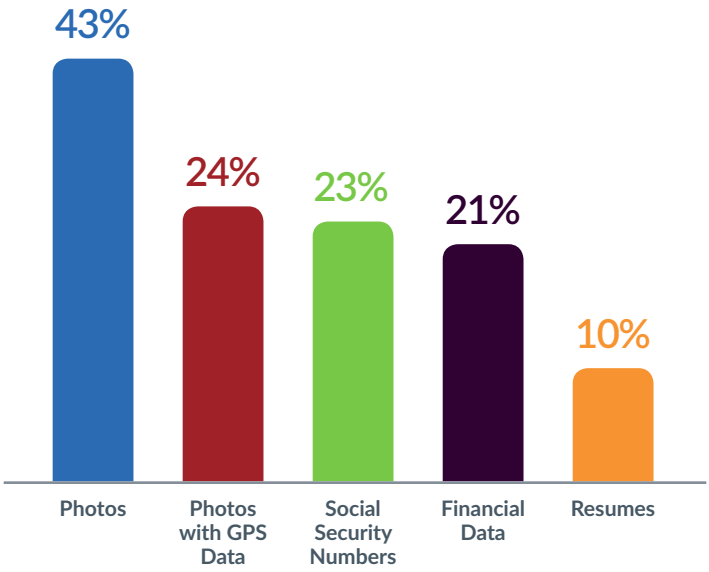
KEY TRENDS & INSIGHTS

Social Security Numbers, Financial Data and Resumes Top List of Personally Identifiable Information Recovered from Used Drives

Over half (67 percent) of the used drives we examined contained personally identifiable information. In addition to finding photos (43 percent) and photos with GPS data (24 percent), our digital forensics experts discovered extremely sensitive information, including financial data (21 percent), social security numbers (23 percent) and resumes (10 percent).

According to our digital forensics expert, Paul Henry, users should be worried if these types of personal information are retrieved. "Two of the more incriminating types of personal information we recovered are financial data and resumes - these types of files contain all of the information needed for a hacker to go in, steal the information and then perpetrate identity theft and fraud. And in a world where money rules, this could have devastating effects for individuals because it could not only rob them of their hard-earned money, but it could also hurt their chances to get approved for financing, mortgage loans and so much more. Not to mention, if the identity thief becomes involved in criminal activities, it could destroy their personal reputation."

Which types of personally identifiable information were recovered from the drives?



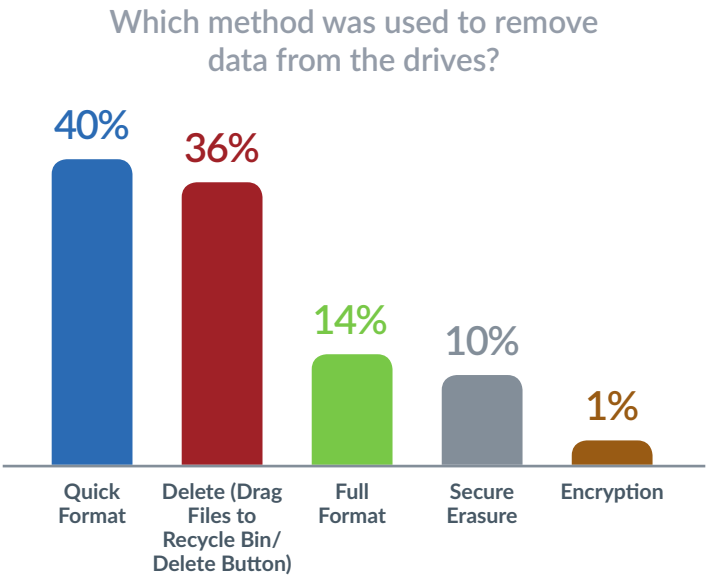
blancco technology group

KEY TRENDS & INSIGHTS

Delete Doesn't Always Mean Delete

Based on our analysis of the 200 used drives purchased from eBay and Craigslist, 36 percent of the drives containing residual data had data previously 'deleted' from them – essentially, users dragged files to the 'Recycle Bin' or used the basic delete button.

As we've seen from previous data security studies and real-world data breaches, most users don't understand the difference between 'delete' and erase. When you talk about deleting files from a laptop/computer, it typically entails hitting the 'delete' button, dragging files to the Trash Bin or reformatting the drive itself. Most people – and even businesses – mistakenly use one or all of these methods thinking their information is gone. But it's not. The data can still be accessed and recovered.



This was evidenced with the infamous Ashley Madison data breach in 2015, when users were led to believe that paying $20 for the dating site's 'Full Delete' service would permanently erase their data. But as the countless news reports revealed, that was not the case and hackers posted the users' account details online, including their real names, usernames, email addresses, profile information, dates of birth, gender, weight, height and even the zip code of their addresses.

Because of how important this subject is – and how little awareness and knowledge there is on the topic – we have outlined below the differences between insecure deletion and permanent removal.

Deleted Files	Permanently Erased Files
Easy & Fast, But Unreliable	Easy, Fast & Reliable
File Recovery Is Possible	File Recovery Is Impossible
Insecure	100% Secure
Increases Risk of Data Loss/Leaks	Prevents Data Loss/Leaks
Uncertified Method	Certified Method
No Proof of Removal	Proof of Removal

Quick Formatted Data Can Still Be Recoverable

As our team found, a quick format was performed on nearly half (40 percent) of the used drives containing residual data. However, formatting a drive doesn't actually erase the data. It only creates a file table so new data can be written to the volume. So the old data is still left intact and recoverable.

When you consider that close to half of the used drives we analyzed used this inadequate data removal method, it reiterates just how large and persistent of a problem this is today. For businesses that collect, create, store and manage millions of data points and information in a single day, the security risks of exposing such data are too significant to ignore.

According to our IT Security Consultant, Paul Henry, users often put their blind faith into quick format and reformatting, thinking these methods will permanently get rid of the data and prevent it from resurfacing. But these methods don't always work.

"For data security as a whole, and data erasure in particular, there are many solutions users can find in the marketplace. But as easy as they are to find and as affordable as they might seem, they're not absolutely guaranteed to erase data permanently – and they certainly don't comply with international regulatory standards. But as our study makes very clear, not all resellers are taking the necessary precautions to wipe data completely clean before reselling used electronics to the next user."

KEY TRENDS & INSIGHTS

Despite Proven Capabilities, Data Erasure Is Still Lesser-Known Unicorn

Out of the 200 used HDDs and SSDs we analyzed, very few (only 10 percent) had a secure data erasure method performed on them. This is both surprising and disappointing because it is the most proven and effective method to completely and permanently erase data. Yet, so few users know about it and even fewer have access to the right technology, resources and budgets to implement it – for themselves personally and for the drives used by their entire workforces, contractors and vendors.

Our IT security consultant, Paul Henry, sees this finding as indicative of the state of data security knowledge today. "All data deletion methods are *not* equally capable of erasing data completely and permanently. But if you ask most people inside your company to first tell you the different types of data deletion methods and then identify which of those methods are adequate and which ones aren't, I'd say less than 10 percent of those people would be able to do this. That's where data erasure sits today in the knowledge spectrum of data security. This needs to change sooner than later."

10%

Out of the 200 used HDDs and SSDs we analyzed, very few (only 10 percent) had a secure data erasure method performed on them.

Data Removal Buck Stops With Original Users/Owners

It's the responsibility of the original user or owner to properly sanitize their equipment before it's traded in, resold, donated or discarded. If individuals simply rely on others to take care of protecting their data, that's just irresponsible. Similarly, if businesses take a lax approach or don't monitor how, when and where all of the data from their equipment is removed before it's discarded, reused or recycled and if they fail to obtain actual verification that all data has been removed permanently, it's just as irresponsible and can cause serious financial, legal and reputational damage.

CONCLUSION

Hard disk drives and solid state drives are often an appealing way to store data because they are durable, cost-effective and reliable. But despite these benefits, many enterprise IT teams struggle with the upkeep of these drives. One of the more troublesome challenges is related to wiping the data from them when employees leave the company, the drives hit their end of life or the data itself needs to be removed to comply with IT policies and security regulations. These challenges are further compounded by budgetary and resources constraints, which have led many organizations to resell and/or reuse drives whenever possible.

However, knowledge of the proper data erasure methods and tools for these drives has not been anywhere near as fast or as ubiquitous as their adoption rates. And when free tools/software are used, it makes matters even worse because such tools cannot adequately do the job and leave large amounts of data accessible.

ABOUT BLANCCO TECHNOLOGY GROUP

Blancco Technology Group is a leading, global provider of mobile device diagnostics and secure data erasure solutions. We help our clients' customers test, diagnose, repair and repurpose IT devices with the most proven and certified software. Our clientele consists of equipment manufacturers, mobile network operators, retailers, financial institutions, healthcare providers and government organizations worldwide. The company is headquartered in Alpharetta, GA, United States, with a distributed workforce and customer base across the globe.

For more information visit:
www.blanccotechnologygroup.com

Blancco, a division of Blancco Technology Group, is the global de facto standard in certified data erasure. We provide thousands of organizations with an absolute line of defense against costly security breaches, as well as verification of regulatory compliance through a 100% tamper-proof audit trail.

SmartChk, a division of Blancco Technology Group, is a global innovator in mobile asset diagnostics and business intelligence. We partner with our customers to improve their customers' experience by providing seamless solutions to test, diagnose and repair mobile assets. SmartChk provides world-class support, pre and post implementation, allowing our customers to derive measurable business results.

CONTACT US

For Sales & Marketing, Please Contact:
Email: info@blanccotechgroup.com

For Corporate Communications & PR, Please Contact:
Email: press@blanccotechgroup.com