blancco
technology group

RESEARCH STUDY

Delete vs. Erase: How Companies Wipe Active Files

September 2016

TABLE OF CONTENTS

INTRODUCTION

According to IBM, 2.5 quintillion bytes of data are created every day. This includes various types of data, including documents and files, digital photos and videos, ecommerce payment transactions, payroll and health records, social media posts, among others.

2.5 Quintillion Bytes

Data Created Daily

There's no doubt data provides a treasure trove of information for businesses and reveals important details about their customers, including demographic profiles, purchase preferences, engagement with content and ads, buying behaviors and so much more. And it's served them well – improving the customer experience across all channels, driving higher brand engagement and recall, boosting digital engagement and increasing product sales and revenue growth.

Over the last several years, we've worked with businesses in the finance, healthcare and government sectors to help them understand the need to permanently and verifiably erase data from IT equipment and devices. More often than not, organizations will consider this necessary when their equipment reaches end of life.

But what about erasing active files on desktop computers, laptops, external drives and servers? This is often overlooked, or altogether forgotten, by businesses. And it's often due to a misunderstanding of the proper data removal methods and lack of access to effective tools so that they can wipe data in their active IT environments. As a result, many organizations are leaving large volumes of sensitive, confidential and potentially compromising data exposed and vulnerable to loss or theft. With over 300 million records leaked and over $1 billion stolen in 2015, it's not a matter of if, but when, organizations will be hit by a data breach. When you factor in that the Ponemon Institute estimates the total cost of a data breach to be from $2.1 million to $6.7 million, it's difficult to ignore the serious consequences of improper data management.

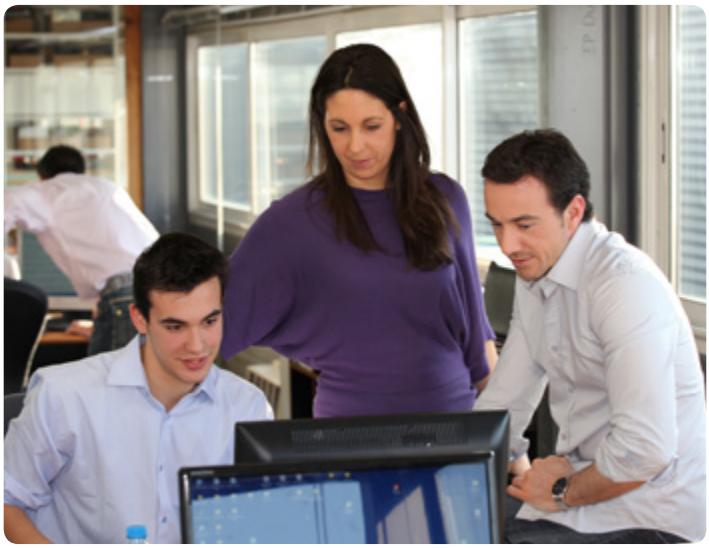
So why are so many organizations not securely erasing files from active desktop computers/laptops, external drives and servers? Historically, IT teams haven't always placed data removal at the top of their IT security priorities, in comparison to what they perceive as more 'threatening' risks such as malware and targeted attacks. Because of this perception and low prioritization, it has been difficult to get buy-in from the C-suite and board of directors to increase budgets, resources and staff to implement the necessary data removal tools and methods.

Our study indicates that erasing data – when IT equipment reaches end of life or from live IT environments – is both complicated and challenging. But as data breaches occur every day with greater consequences, data removal seems to be inching up the list of IT security priorities for organizations around the world.

SURVEY METHODOLOGY & OBJECTIVES

We surveyed over 400 IT professionals in the United States, Canada, Mexico, United Kingdom, France, Germany, Japan, China and India to understand how companies manage user groups and endpoints through Microsoft Active Directory, how active files are removed in live environments from desktop/laptop computers, external drives and servers, their knowledge and understanding of file removal methods and key challenges they face in these areas.

The survey was fielded in July 2016 and the respondents are comprised of adults, aged 18-65 years old, who work in IT decision-making roles at organizations in the retail, healthcare, transportation, banking/financial, government/public sector and manufacturing industries.

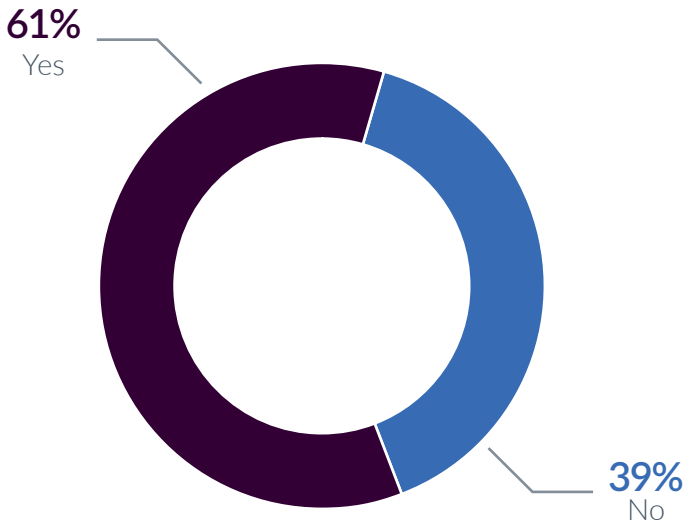


SURVEY RESULTS & DISCUSSION

Microsoft Active Directory Is Preferred Tool for Automating File Management

Based on our study's findings, 61 percent of IT professionals use Microsoft Active Directory to manage files/folders. This indicates AD's value and role in helping IT teams automate their file management and control access rights, user groups and endpoints. If you ask Microsoft's Director of Program Management for Active Directory, Alex Simons, he would estimate that 90 percent of companies are running Active Directory – totaling close to 500 million active account users. But even Microsoft itself understands that AD's value doesn't eliminate the need for proper data management and security practices. At the 2015 Cloud Identity Summit, Simons admitted "95 million of those accounts are under attack every single day."

Does your company use Active Directory to manage files/folders?



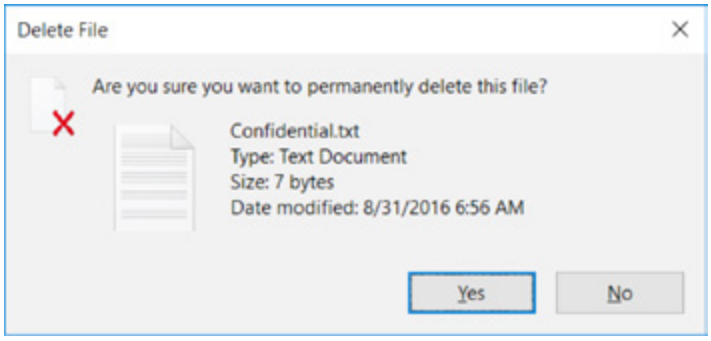
SURVEY RESULTS & DISCUSSION

It's Easy to Confuse Deleting & Erasing Files

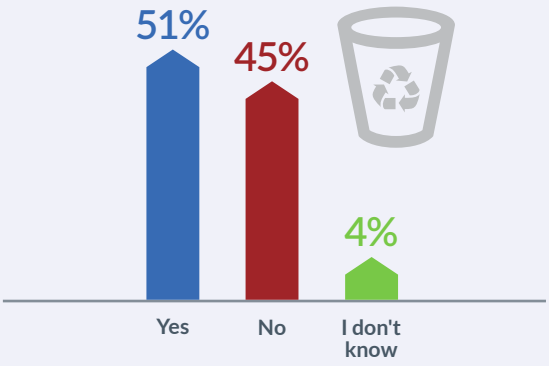
According to our study's findings, over half (51 percent) of the respondents believe files are permanently gone when they empty the Recycle Bin on their desktop computers/laptops. And another 51 percent believe performing a quick format and/or full reformat of a computer's entire drive is sufficient to permanently erase data. As you can see, it's not always easy to tell the difference between 'deleting' and 'erasing' data.

As our CEO Pat Clawson recently explained in an interview with Fast Company, "Part of the problem is that the tech industry hasn't always made it easy for users to figure out how to delete their information, and hasn't made clear the difference between secure erasure techniques—where data is actually overwritten on a storage device multiple times to render it truly unrecoverable—and quicker modes of deletion where disk space is merely marked as reusable."

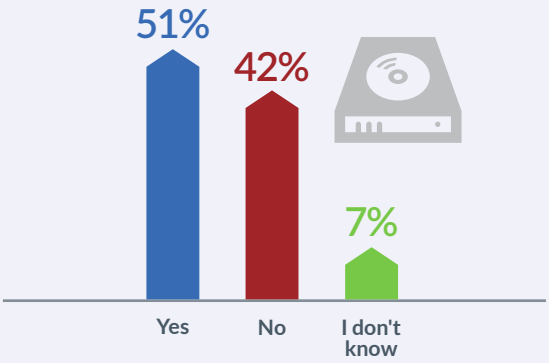
It's no wonder so many IT professionals believe dragging files to the Recycle Bin on their laptops/desktop computers wipes them clean because Windows prompts them with the following question on the screen: "Are you sure you want to permanently delete this file?" But in fact, only the pointers to those files are deleted, leaving the underlying data in place. This misleads users to believe that the file is permanently erased. However, that is not the case. We know from our recent data recovery study that basic deletion only removes pointers to the data, not the data itself, and leaves data recoverable and vulnerable to a data breach.



Once you empty the Recycle Bin on desktop computers/laptops, are those files permanently gone?



Does performing a quick format and/or full reformat of a computer's entire drive permanently erase all data so it can never be recovered?



SURVEY RESULTS & DISCUSSION

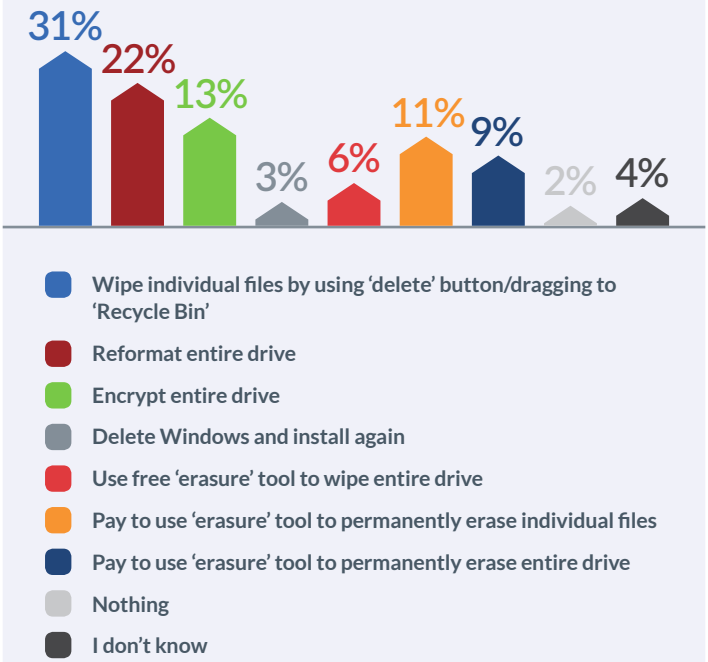
Reformatting Drives & Basic File Deletion Increase Exposure to Security Risks

When we asked IT professionals how they wipe files from company-owned laptops/desktop computers, 22 percent said they reformat the entire drive. Additionally, 31 percent of the surveyed IT professionals said they wipe individual files by using the 'delete' button and dragging the files to the Recycle Bin. Combined, that's 53 percent of IT professionals who are using two ineffective and insecure methods to wipe active files.

According to our findings, this is happening frequently. In fact, 77 percent of the respondents said they hit the 'Delete' button and/or drag files to the Recycle Bin on their laptops/desktop computers at least once a week to as often as six to 10 times a day. This should be cause for alarm for all organizations, given the fact that reformatting drives doesn't overwrite data a sufficient number of times and thus, leaves the data intact and easily recoverable through free data recovery tools. And even overwritten files do not meet the required regulatory obligations.

Now consider this: 6 percent of IT professionals either use 'nothing' or 'don't know' how they wipe active files. While this percentage is not extremely high, it represents an opportunity to better understand how data removal works and the right tools to ensure data is erased in accordance with regulatory requirements. If you consider the average organization owns thousands of desktop computers and laptops, that means a massive volume of sensitive files could be sitting on them and easily be lost or stolen – all because improper data removal methods were used.

How do you wipe files from company-owned laptops/desktop computers?



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

How often do you hit the 'Delete' button and/or drag files to the Recycle Bin on company-owned laptops/desktop computers to get rid of files?

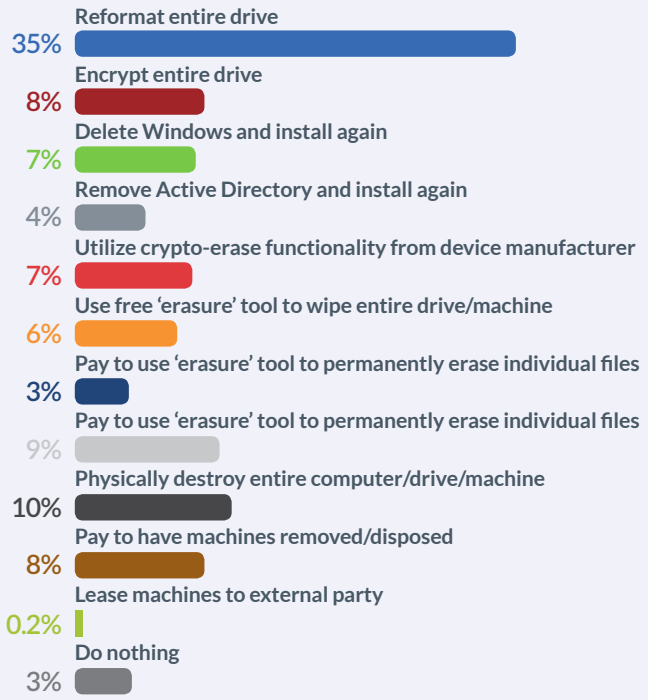
Note: Figures may not add to 100 due to rounding.

SURVEY RESULTS & DISCUSSION

Storage and Handling of IT Equipment Are More Important Than You Think

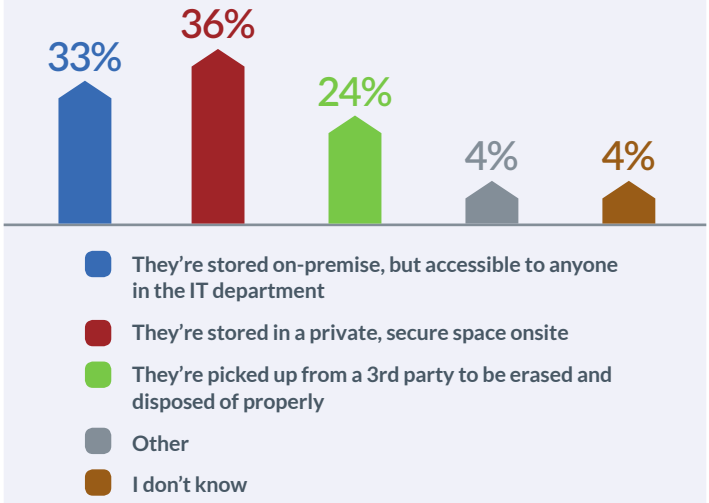
In June 2015, 12 U.S. state agencies in Massachusetts responsible for handling taxes, programs for people with mental illness and drivers licenses were audited and cited for improper storage and destruction of sensitive computer records, thus violating data security requirements. At the Office of the Chief Medical Examiner, for example, electronic equipment that may have contained confidential information was stored in areas 'easily accessible' to people outside the office's information technology department. Additionally, 40 hard drives that had been designated as 'worthless' were left in an open, unsecured area.

When your company disposes of, recycles or resells old desktop computers, laptops, external drives and physical servers, how do you wipe them clean of all data?



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

Where does your company store desktop computers, laptops, external drives (HDDs and SSDs) and physical servers that are no longer in use/functional?



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

But as our study indicates, improper storage and handling is a bigger data security problem and risk than organizations might realize. In fact, 33 percent of the respondents said their companies store old/non-functional desktop/laptop computers, external drives and servers on-premise in locations that are accessible to anyone in the IT department. Meanwhile, 4 percent said they don't even know where this equipment is stored.

Since we previously revealed that a large portion of IT professionals are using basic file deletion and reformatting to wipe files from company-owned laptops/desktop computers, it's even more important for those organizations to properly store and handle their IT equipment so the risks to data are not further exacerbated. In addition to putting corporate data at risk, organizations could also find themselves in a similar auditing situation as the 12 U.S. state agencies in Massachusetts that failed to comply with data security requirements.

SURVEY RESULTS & DISCUSSION

The Fear of Losing Intellectual Property and Login Credentials Is Very Real

In the last few years, data breaches have become a common fact of life. For organizations like Sony Pictures and Mossack Fonseca (of Panama Papers fame), the impact of the data breaches has been far-reaching and resulted in the loss of sales, diminished customer loyalty, regulatory fines and lawsuits, not to mention a whirlwind of negative publicity and backlash from frustrated customers. A key reason why the aforementioned data breaches had such a tremendous impact on the businesses is that the breached files contained confidential information, intellectual property and, in some instances, compromising details about business dealings and sensitive communications.

According to our study's findings, organizations are worried about losing intellectual property and confidential information. To be exact, 14 percent of the surveyed IT professionals are most concerned with securing confidential product development materials, followed by company revenue statements (12 percent), customer contracts (11 percent), usernames and passwords to the company intranet (10 percent) and login credentials to company systems and portals (9 percent).

SURVEY RESULTS & DISCUSSION

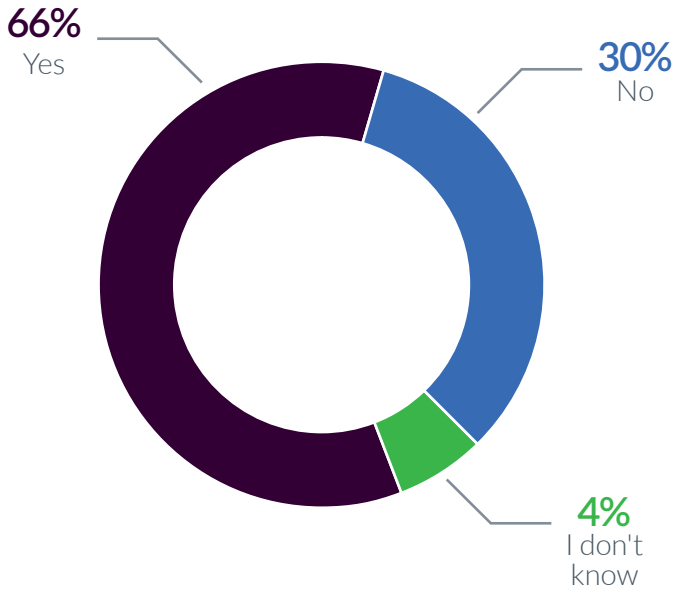
Data Retention Policies Need Better Oversight and Enforcement

Data retention policies help organizations maintain various types of data for a pre-determined period of time. And depending on the classification of data and regulatory requirements, different types of data must be retained for different periods of time. But data retention policies don't only focus on the retention period. When done right, they specify the procedures for managing data across each stage of its lifecycle, destroying data when it's no longer required to be held as well as establishing enforcement mechanisms to ensure data is managed and removed properly in accordance with regulatory requirements.

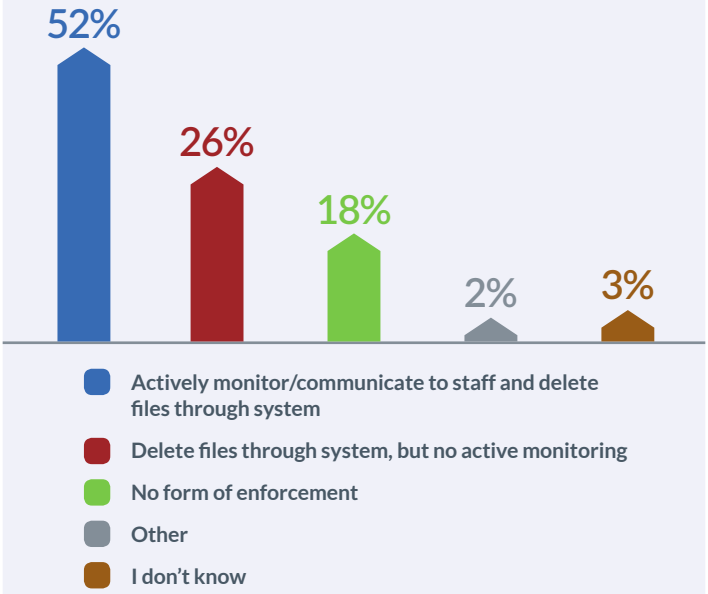
As our study indicates, nearly one-third of organizations (30 percent) do not have written data retention or removal policies in place. Furthermore, our findings indicate there is very little oversight into data retention policies with enforcement mechanisms rarely present. More specifically, 26 percent of the surveyed IT professionals confirmed they delete files through the system, but admitted to having no active monitoring in place. Plus, another 18 percent have no form of enforcement in place at all.

Organizations need to prioritize data retention and removal to protect their corporate, customer and employee data. But it has to go beyond just creating data retention policies. To protect sensitive data from being breached, organizations must put just as much onus on the enforcement of their data retention policies. Without regular oversight and enforcement mechanisms, it's difficult to guarantee that data retention policies will actually be implemented.

Does your company have written data retention or removal policies in place?



How does your company enforce written data retention or removal policies?



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

SURVEY RESULTS & DISCUSSION

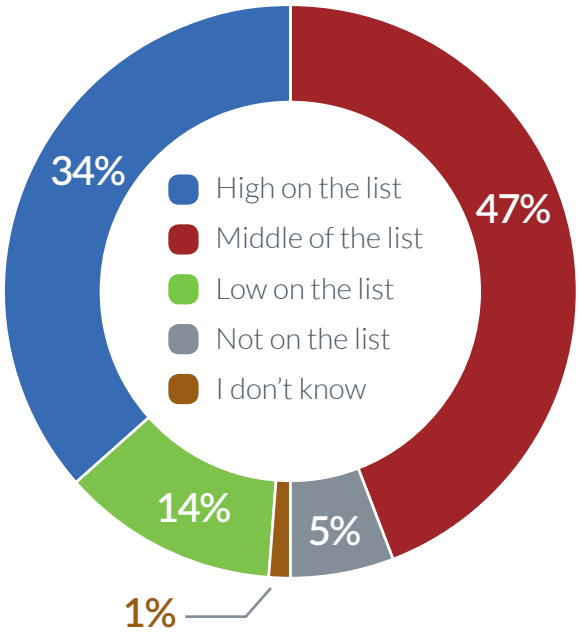
Data Removal Is Inching Its Way Up List of IT Security Priorities

Historically, data removal has not been given as much weight or priority among IT professionals in comparison to other more serious data security threats, such as malware, extortion hacks, backdoor attacks and accidental insider threats. But according to our study's findings, this may be changing.

When we asked IT professionals to rank a variety of security threats in terms of risk level to their organizations, the responses were surprising. Incomplete/improper data removal ranked the highest, at 9.44, compared to backdoor attacks (6.17), extortion hacks (6.42), malware (6.23) and accidental insider threats (6.60). On top of that, over one-third (34 percent) of the respondents said data removal is high on their overall list of IT security priorities and 47 percent place it in the middle of their priority list.

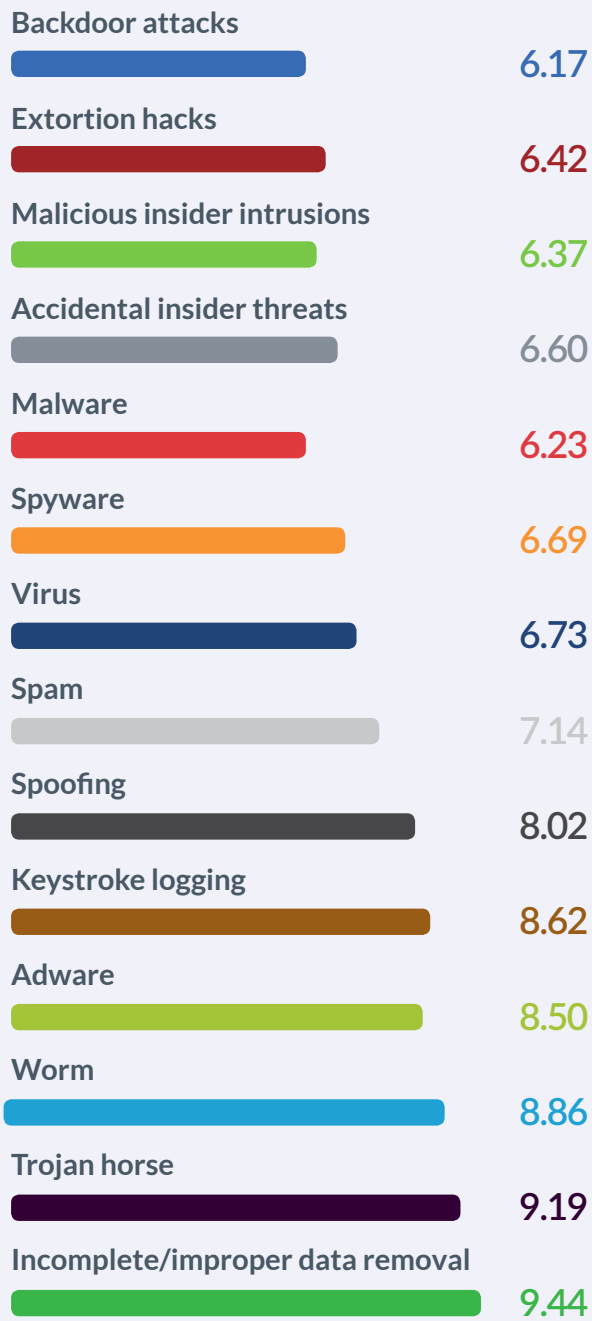
These are positive signs for the state of data security and privacy. It suggests that organizations may be starting to change the way they think about and approach how data is managed across its entire lifecycle – from creation to collection to storage to archival to transfer to destruction.

Where does data removal fit into your company's overall list of IT security priorities?



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

Rank the following computer security threats in terms of risk level to your organization. (1 means 'lowest risk' and 14 means 'highest risk')



CONCLUSION

Cyber attacks and data breaches have become a common and unfortunate reality in today's digitally connected world. But there is no single technique or solution that can guarantee 100% data protection. Security risks are often exacerbated in live environments due to the fact that users often don't understand the difference between insecure and secure deletion methods, such as dragging files to the Recycle Bin and reformatting drives. As a result, sensitive files often sit exposed and vulnerable to loss/theft on IT equipment, such as desktop computers/laptops, external drives and servers.

However, if data is actively removed securely and permanently on a regular basis based on data retention policies, organizations can add an extra layer to their overall security program and ensure compliance to the most stringent security regulations around the world.

To help organizations get started, we developed a tips sheet with 6 important rules to follow when erasing files through Microsoft Active Directory.

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