DISPUTES AND INVESTIGATIONS

THE RISKS OF LEFTOVER DATA: A RECOVERY STUDY

A&M's forensic analysis of computers unveils the dangers of inadequate data disposal for individuals and businesses

Introduction

The rise of bring-your-own-device (BYOD) and remote working are increasingly blurring the lines between personal and business use of devices, which exacerbates existing concerns around data security and the lifecycle management of IT assets.

This hybrid environment brings new challenges for organisations, including reduced capability to monitor staff working virtually and the inability to make sure data is handled and destroyed. Firms may also find it more difficult to fully regain access to relevant systems to ensure sensitive data is securely and comprehensively wiped after a remote worker leaves the business. In addition, work-from-home (WFH) arrangements have led to a rise in IT equipment being lost or stolen[1], the chief cause of data theft.

Failure to properly dispose of redundant IT equipment can lead to data breaches that not only violate data protection laws but can also result in financial fraud, with devastating impacts on companies' finances and reputation. For individuals, there is the risk of identity theft if personal information falls into the wrong hands, causing monetary losses and serious emotional distress.

To expose the dangers of inadequate data disposal in business and private settings, Alvarez & Marsal's Disputes and Investigation team conducted a forensic analysis of six used computers that were available for sale on an online marketplace.

Using forensic technology software and e-Discovery tools, we were able to recover thousands of documents from the computers, including hundreds with highly sensitive personal information, as well as a significant amount of business-related data.

This report summarises key findings of the analysis and discusses the best practices in data destruction policy to help companies and individuals avoid data breaches and falling victim of fraud.

A&M's Forensics Analysis – Step by Step

1 Devices were imaged via forensic technology software in our lab

2 Each image was passed through forensic analysis software to attempt to recover deleted data , a process known as carving

3 Relevant data were then processed to allow for further analysis and searching; documents of interest were marked

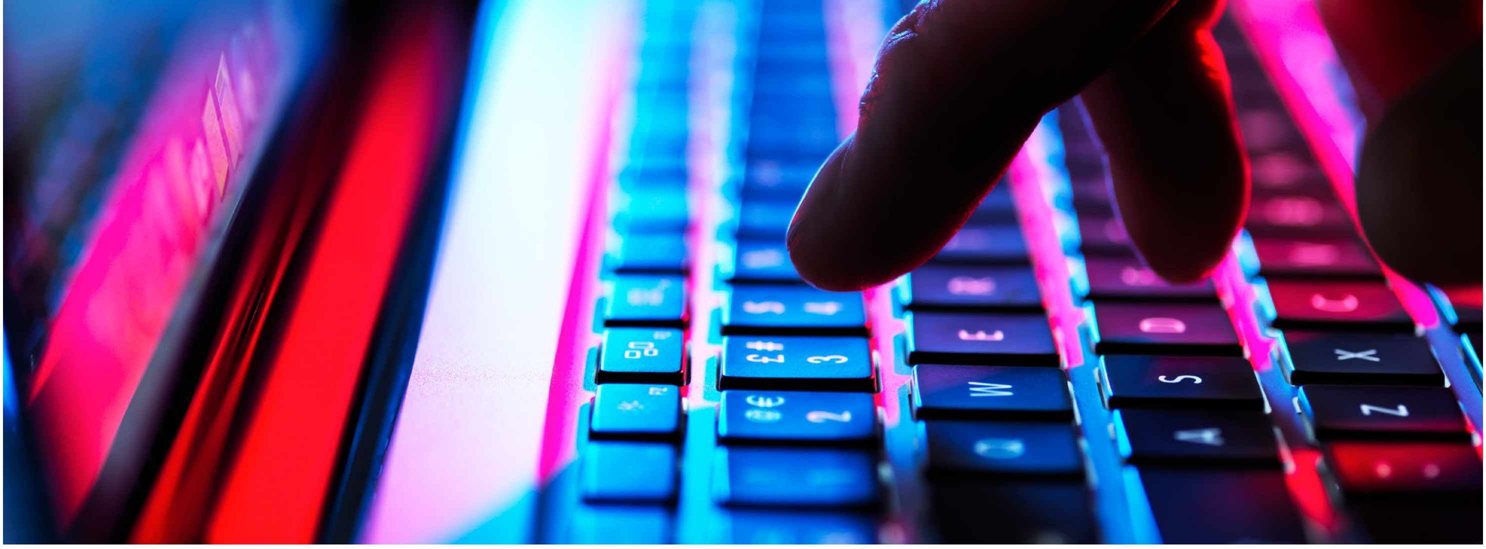
Analysis and Methodology

In the first half of 2022, we purchased six computers over the e-commerce platform eBay in the U.K. We bought a mix of personal and what appeared to be previous work devices[2], focusing on those where there was no statement about them being securely wiped.

Our analysis found data on five of the six computers. In addition, we were also able to retrieve data from some computers that were not fully deleted from the hard drive, suggesting that the previous owner had attempted some form of cleansing but that it was not 100% effective. In other cases, data had not been erased at all, and we were simply able to identify information that was live on the machine.

[1] https://www.fraudscape.co.uk/

[2] Defined as computers which had asset tags and appeared to have leftover stickers/markings indicating that they were tagged by a company as part of an inventory process.



It is also worth noting that the data was captured using software that is available to anyone with the right knowledge (e.g. not exclusive to law enforcement agencies), highlighting its vulnerability to fraudsters and other malicious actors with moderate forensics skills.

The data was then analysed using forensic technology software enabling us to recover deleted files and performed data categorisation to paint a clear picture of the data on the computers.

The information discovered was subsequently processed to enable linguistic clustering to be performed, which identifies certain themes that appear more frequently within the data and grouping the content of the files around those themes.

Top Findings

In total, our forensic analysis was able to recover 5,875 user-generated documents across the six computers. Several documents came from carved data — that is, deleted data on the hard drives of the computers — with a few documents still sitting on the computers, undeleted.

The majority of the data recovered contained personal information, including clear scans of an in-date passport and various appraisal and job application forms detailing personal identifiable details such as full names, National Insurance numbers, addresses, emails, dates of birth and other sensitive data. Personal photos were also found among the data.

Additionally, 366 files included work-related keywords. These keywords were derived from both generic business terms and concepts we discovered during the clustering process.

For example, 155 documents had references to “invoice,” 100 to “court,” 44 to “bailiff” and 23 to “applicant.” A further 84 files contained the keyword “report” and 23 mentioned the word “appraisal.” We also found images of building identification cards, salaries of employees, invoices and other internal business correspondence.

Computer Forensic Analysis - Highlights

- 5,875 documents were retrieved from the PCs
- 366 files included work-related keywords
- 4% contained residual data that had been improperly deleted
- Web-related items accounted for 16% of overall data
- 2,111 email items were found
- Social networking, location and travel data were also found

Key Insights

1. Personal Data Presents the Highest Threat

Perhaps unsurprisingly given that the second-hand computer market is dominated by individual sellers and buyers, personal data accounted for the majority of the data recovered by our team in the study.

We were able to find highly sensitive information such as passport numbers, emails and addresses, representing a significant risk of identity theft.

Criminals can use stolen personal information such as the kinds we found to make card applications, open bank accounts or apply for state benefits. Thieves can also use the data to stalk and blackmail, causing severe mental distress to the victims. Identity theft cases have been on the rise recently, with cases in the U.K. rising 22% in 2021 to 226,000, constituting 63% of all fraud cases recorded to the U.K.s National Fraud Database.

2. But Risks Extend to The Business World Too

While only 6% of the files recovered in the analysis contained business-related information, the very fact that they made their way onto the personal devices is worrying.

If released into the wrong hands, even what appears to be small, harmless data can create devastating effects to companies. Some of these risk implications include:

- Violation of data protection laws: data destruction is a critical element of data protection laws. For example, in the case of EU's GDPR, unnecessarily holding on to personal data runs the risk of greater fines and likelihood of enforcement if this data is involved in a privacy breach. Failing to comply can trigger legal proceedings and significant fines.
- Data breach and business fraud: unsafe data disposal practices leave organisations vulnerable to data breaches, putting customers, suppliers, employees and the business at risk. Leakages can lead to frauds with significant financial costs and reputational damage.
- Theft of sensitive business information: the exposure of IP data, employee wages and internal communications can lead to internal conflict, damages to reputation and competitive advantages as well as to financial losses.

3. Best Practices in Data Disposal Policy

To mitigate the risks outlined above, we recommend companies consider the following best practices in data disposal management:

a. **Heavily enforce data security policies**. To prevent sensitive data from being transmitted outside of secure environments in the first place, company emails and documents should ideally be saved to the cloud as these storage locations are generally more secure than a computer hard drive. Employee training and access is also critical to data security as most data leaks come from human error.

b. **Establish and maintain a secure data destruction policy**. Organisations have a responsibility to only collect data that they need from their customers and employees and to only hold it for as long as necessary to meet these lawful purposes. This means that companies need to understand the data they hold and put in place not just policies around usage, retention and the effective deletion of data, but also technical and organisational controls, including compliance monitoring, to ensure that these requirements are met in practice.

c. **Adapt policies for the new business reality**. Data disposal policies must be updated to reflect the current BYOD/WFH environment. New considerations should include how to ensure devices are handed back when an employee who works remotely leaves the firm or how to remotely wipe IT assets if they refuse to return devices or in case of loss/theft/replacement. One alternative is to create incentivised pathways for staff to dispose of electronic devices responsibly.

d. **Ensure all data is securely and effectively wiped.** Deletion and formatting — including factory resets — do not permanently remove the data from the devices, as our analysis showed. Therefore, zeroing out a hard drive, or forensically wiping it, is the best way to sanitise a device so data cannot be recovered by hackers. This can be done using specialist software tools, such as the ones we used in this analysis, but free tools can also offer a good level of sanitisation. Physical shredding of hard drives is also recommended.

e. **Audit third-party technology providers for secure deletion of data**. Even when a company uses third-party technology providers or outsources all or some of its data management services, the obligations to comply with relevant data protection laws remain with the company. Appropriate technical, operational and legal measures must be in place with all vendors and service providers processing personal data. This may include having certified and audited procedures governing the secure deletion of data and destruction of hardware devices.

How Can A&M Help?

A&M's forensic analysis of six used computers revealed the risks of inadequate policy for data disposal and destruction. More than 5,800 documents were retrieved from the computers, including sensitive personal information and business-related data. In some instances, data was able to be retrieved with relative ease by using widely available forensic software.

A&M's Disputes and Investigations digital forensics and privacy specialists can help companies revise policies and procedures as well as implement risk assessments to gauge how vulnerable they are to those risks. We can also advise on practical steps to be taken in order to make data more secure and prevent it from falling into the wrong hands.

A&M: Leadership. Action. Results.SM

A&M's Disputes and Investigations professionals draw on their expertise in disputes, investigations and compliance, economic consulting, forensic technology, cybersecurity and data privacy risk, and expert testimony to provide clients with independent and highly qualified advice.

Our experience provides us with a unique ability to articulate complex findings in a clear and meaningful manner and we set the standard for delivering results on critical matters involving corporate investigations, regulatory enforcement actions and high stakes litigation and arbitration. Our experts and investigators work all around the world in North America, Europe, Asia and the Middle East and are experienced in working with outside counsel, boards of directors, audit and special committees, fiduciaries (examiners, monitors, trustees, etc.) and with the management team of public and privately-held companies.

KEY CONTACTS

Phil Beckett
Managing Director

pbeckett@alvarezandmarsal.com

Robert Grosvenor
Managing Director

rgrosvenor@alvarezandmarsal.com

Graeme Buller
Director

gbuller@alvarezandmarsal.com

Danny Lewis
Analyst

danny.lewis@alvarezandmarsal.com

ABOUT ALVAREZ & MARSAL

Companies, investors and government entities around the world turn to Alvarez & Marsal (A&M) for leadership, action and results. Privately held since its founding in 1983, A&M is a leading global professional services firm that provides advisory, business performance improvement and turnaround management services. When conventional approaches are not enough to create transformation and drive change, clients seek our deep expertise and ability to deliver practical solutions to their unique problems.

With over 6,000 people across five continents, we deliver tangible results for corporates, boards, private equity firms, law firms and government agencies facing complex challenges. Our senior leaders, and their teams, leverage A&M's restructuring heritage to help companies act decisively, catapult growth and accelerate results. We are experienced operators, world-class consultants, former regulators and industry authorities with a shared commitment to telling clients what's really needed for turning change into a strategic business asset, managing risk and unlocking value at every stage of growth.

To learn more, visit: **AlvarezandMarsal.com**

Follow A&M on:

411136-25007/Sept 22