

Russell Richardson

Shredding: Waste Versus Security

Why the management of confidential shredding needs to be transferred
from waste management to security

Whitepaper
January 2012

Contents

1. An overview	Page 3
2. What does shredding mean to the average business?	Page 3
3. High levels of security are important to every business	Page 4
4. How did shredding get placed in the wrong sector?	Page 5
4.1 The differences between waste processors and secure shredding suppliers	Page 6
5. Why is it important to securely dispose of information?	Page 7
5.1 Data Protection Act compliance	Page 7
5.2 Corporate identity theft	Page 8
6. Key elements that make a shredding service secure	Page 8
7. Methodology for transferring shredding to a security function	Page 9
8. Conclusion	Page 10
9. About Russell Richardson	Page 11

Diagrams

4.1 Typical confidential document destruction process	Page 5
7.1 Simplified methodology for transferring shredding to the security function	Page 10

Shredding: Waste Versus Security

Why the management of confidential shredding needs to be moved from waste management to security

1. An overview

The aim of this whitepaper is to offer readers with an explanation of why shredding has been placed into the wrong sector and provide a straightforward methodology for transferring shredding into the security department. Designed to be practical and informative, it also seeks to give guidance with regards to the necessary security accreditations that a shredding supplier should possess.

2. What does shredding mean to the average business?

Shredding is the process of cutting paper into either strips or fine particles, but for the purpose of this whitepaper it will refer to industrial strength shredding equipment that can process up to 2,500kgs per hour and even shred material, packaging and computer hard drives.

Standard practice is for businesses, organisations and government departments to only shred those documents that they consider private, confidential or to contain sensitive information as this is the only requirement that is currently enforced by UK law (Data Protection Act (DPA)). Unfortunately, it is often wrongly assumed that document and information destruction can be dealt with effectively via internal measures, such as desktop shredders or the general waste collection service. Even in the smallest organisation, internal methods for disposal and destruction of any documents are simply not adequate.

In cases where shredding is undertaken internally, it is often the responsibility of the office manager or administration person to decide on what is confidential and shred it. The typical reason behind this practice is for cost saving but it can often be a false economy as the member of staff still needs to be paid for their time physically shredding and make the decision what to shred and what goes in the general waste bin. It can only take one wrong decision over what is classified as confidential and what isn't, for a

company to be in breach of the DPA. Furthermore, is the member of staff even aware of the different facets of the DPA, or the consequences of non-compliance?

Where shredding is outsourced, third party cleaning staff have even been given the responsibility of shredding all the documents marked as confidential, as it is viewed as a waste product. While this throws up a number of issues, the main concern would be that of security, first with regards to the initial storage of confidential documents prior to destruction and more importantly, whether the cleaning staff are security vetted with background checks? Security clearance is not standard practice for cleaning personnel so it should be assumed that they are not and therefore, are compromising the overall security of the business.

3. High levels of security are important to every business

The volatile nature of the current economy requires that every business must effectively safeguard its future, from the obvious physical security of staff, premises and stock to the protection of intellectual property. Even document management needs to be taken seriously in order to keep an organisation and its procedures secure. However, it can often be the less obvious processes, such as the disposal and destruction of confidential information or documents that if not robust enough can leave a business vulnerable not just to breaches of the DPA but also criminal activity.

For example, consider what happens to general commercial rubbish or waste once it leaves an organisation's premises. How many people are involved in the disposal process and have the opportunity to see and remove potentially confidential, sensitive information or branded materials prior to its final destination, landfill? A standard commercial waste collection service will not have security at the top of its agenda.

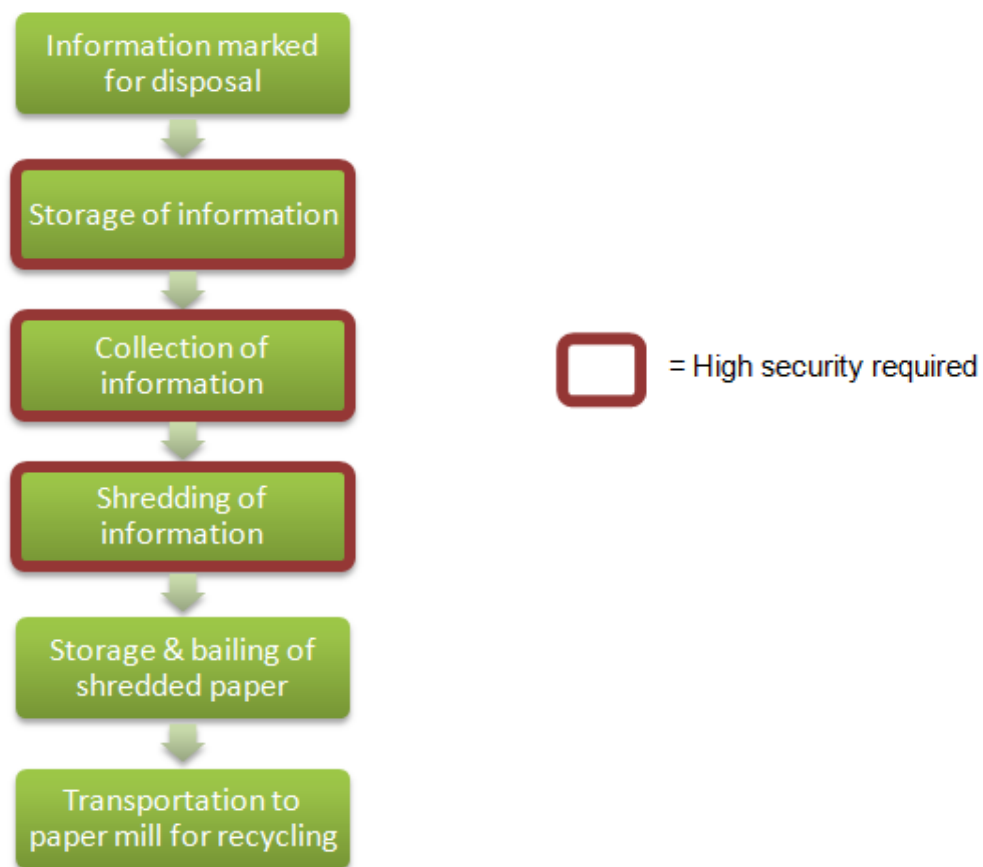
To protect a business, its brand and information created, generated and managed by it, the disposal and destruction of these materials needs a high level of security. Why is it then that the shredding of information, documents, packaging, uniforms etc has been placed in the waste management sector rather than security?

4. How did shredding get placed in the wrong sector?

The main issue appears to be that shredding has been categorised by its main output, waste rather than its secure process. Let's put aside recycling practices for a moment, as traditionally, most people associate waste paper as being thrown into a wastepaper bin (even the name further strengthens the association). Rarely do we consider what happens to that piece of paper after it is put into the bin and the security levels of the disposal process before its final destination, landfill.

In general terms, not many people consider waste paper to hold any value, but what we are failing to recognise is that the information on a piece of paper does have a value. As well as representing an asset, information imposes certain liabilities on an organisation. The security and risk of this liability requires proper and robust management. Disposal and destruction of information is one of the most important elements of document management and needs to be treated as such.

Diagram 4.1 below shows the typical confidential document destruction process



Therefore, the security of the physical shredding (and destruction) is the most important part of the process and not the final product, waste paper or even the eventual recycling. Essentially document shredding companies are selling the secure nature of the process that they undertake and not just the physical act of shredding. However, perception within the general business community continues to be that document shredding companies are waste processors.

4.1 The differences between waste processors and secure shredding suppliers

While to the untrained eye a waste processor and a secure shredding supplier may appear to be similar, this in fact is not the case and there is a vast difference between the two. Section six of this whitepaper provides more in depth information on the specific security accreditations required of a secure shredding supplier but this section is intended to help identify the immediate differences.

In essence a waste processor is a company that will collect many different types of commercial waste from wood, plastics, glass and food to specialist chemical waste. While the service provider will often provide receptacles for the storage of waste materials prior to collection, there is little, if no consideration given to security. And this is evident throughout the entire process as there is often no real requirement for glass bottles or food waste to be kept secure. What's more while a waste processor may in some cases be able to provide details of the amount of waste produced for auditing and recycling purposes, it will be no means be accurate or stand up to close scrutiny.

On the other hand, a secure shredding company has to abide by UK law, namely the DPA, so as a result works with robust procedures in place at every stage. High security is a top priority, from storage of documents prior to destruction, to employees, transportation and even high security shredding facilities.

The issue of misclassification is further compounded as many waste processing companies have diversified into providing a confidential document shredding service without the necessary accreditation. That said, it is acknowledged that there are certain benefits to dealing with one supplier that can process many different waste streams.

5. Why is it important to securely dispose of information?

There are some extremely serious repercussions for those companies that do not comply with the legal requirements (DPA) by disposing of confidential information in a secure and robust manner, as is explained in section 5.1.

However, it is not just breaches of the DPA that can have a detrimental effect on an organisation but also there is the potential to be a victim of corporate identity theft. With the capacity for innumerable ramifications, destruction of not only confidential information but all branded material is essential to prevent it from falling into the wrong hands.

5.1 Data Protection Act compliance

In the UK, the Data Protection Act (DPA) is the official legislation that covers the disposal of confidential documents. In short it states there are a number of legal obligations that companies must comply with in order to protect personal information about individuals and these apply to the processing of personal data. In broad terms, if you use, disclose, retain or destroy information about an identifiable living individual then you must comply with the DPA.

The DPA has eight principals of which two apply to the disposal of personal information. These state that personal data shall not be kept for longer than is necessary and measures shall be taken against unauthorised and unlawful processing of personal data. The Information Commissioner's Office (ICO) regulates compliance with the DPA and has powers which include criminal prosecution, non-criminal enforcement, audit and the power to serve a monetary penalty notice of up to £500,000.

While at the present time there is no random proactive inspection process from the ICO, ignorance is not an acceptable excuse and business owners should have an understanding of the DPA or alternatively outsource to a trustworthy and accredited partner.

5.2 Corporate identity theft

Corporate identity theft is a growing issue for businesses of all sizes across the UK but particularly small and medium enterprises (SMEs). It is defined as the fraudulent impersonation of an organisation for financial gain. Many corporate identity crimes begin with fraudsters changing key company information, such as address or registered directors' names, information that is pretty simple to get hold of. The rubbish bins of an office will herald more than enough information for corporate identity theft to be undertaken, and it is not simply financial information but all branded materials, including packaging, old uniforms or identity badges that need to be destroyed in a secure manner.

Companies House states that there are up to 100 cases of corporate identity theft every month, in reality this figure is likely to be much higher. Once fraudsters are in possession of these basic details, criminal activities can soon spiral out of control with those responsible trading illegally under the company's name and brand, ordering goods, withdrawing funds from business bank accounts and applying for credit facilities. All of this can have a profound effect on a company's reputation with suppliers, customers, clients and at the extreme end even put a company out of business.

It has been estimated that losses due to corporate identity theft can reach the region of £15,000 for an individual company, with figures of up to £30,000 not being uncommon. However, awareness amongst CEOs of both the effects and more importantly how to effectively safeguard a business against corporate identity theft is still worryingly low.

6. Key elements that make a shredding service secure

Security is of paramount importance when seeking to appoint a shredding provider to dispose of your confidential and branded materials. The only way of guaranteeing high levels of security is to make sure the shredding supplier is suitably accredited. As minimum they should operate to ISO9001:2008 incorporating BS EN15713:2009, the European standard for the destruction of confidential information and its customer service operators should be uniformed, carry formal ID and vetted to BS7858, a 10 year background check. A more superior supplier will hold membership to associations, such as BSIA (British

Security Industry Association) and NAID (National Association for Information Destruction) Europe, ensuring the highest standards of service and ethics are met.

Another key consideration is the storage of information once it has been selected for disposal but prior to destruction. A fully accredited shredding supplier will be able to provide a choice of lockable consoles or bins and confidential shredding bags, that are destroyed with the shred, to keep information secure.

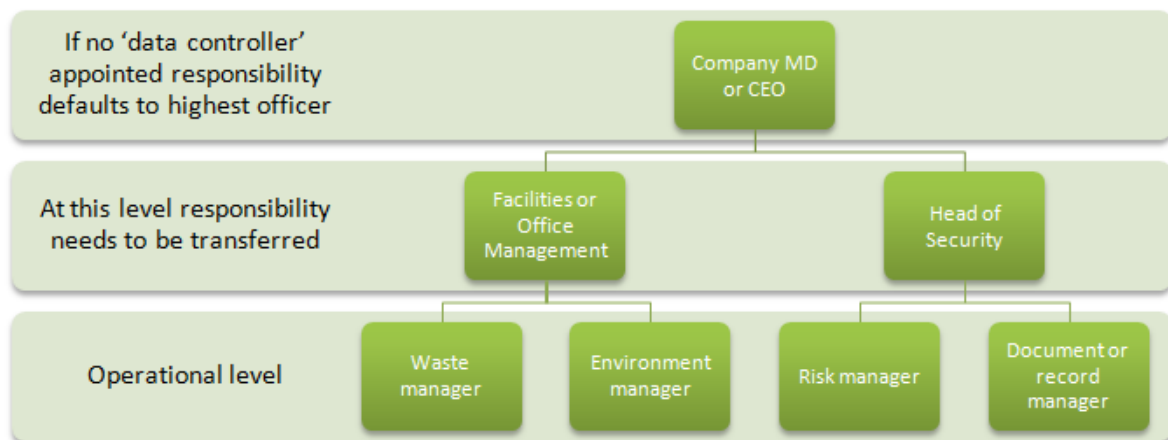
Furthermore, by using legal for trade scales, the supplier can provide a very accurate figure for the amount of shredding conducted and subsequent to the actual shred process will deliver a comprehensive certificate of destruction. This official documentation also provides a robust audit trail which is another necessity for DPA compliance. It has a number of benefits, first there is an audit trail for destroyed information and second it can provide a benchmark for service levels.

Finally, a fully accredited shredding supplier should have no issue with anyone witnessing the entire shredding process or visiting their premises at any point.

7. Methodology for transferring shredding to a security function

All the confusion and misclassification within the shredding industry has made it difficult to precisely pinpoint the job title of the person responsible for document management, disposal and destruction. According to the DPA if no 'data controller' is appointed within an organisation then responsibility for compliance automatically defaults to the highest executive officer, usually the MD or CEO. Logically it would make sense then for the MD or CEO to hold overall responsibility but this is rarely the case.

Diagram 7.1 represents a very simplified methodology for transferring shredding to the security function



Obviously in SMEs there simply will not be this level of hierarchy, so in these instances it is recommended that the responsibility is kept at director level, with specifically appointed and trained personnel directly beneath them. It is also recommended that budgets for shredding are specifically allocated from security as opposed to waste management.

8. Conclusion

Adhering to the law and protecting a business from corporate espionage can be a straightforward process and it is hoped that this whitepaper is a useful tool to help businesses make decisions about shredding and document management with confidence.

At this point it is worth pointing out that a superior shredding partner will undertake a free appraisal of a company's current situation before providing any shredding service proposals. Furthermore, a provider whose mobile shredding trucks feature legal for trade scales will be able to monitor the amount of paper produced. This information can be used to determine whether the service level is correct or if more consoles are required or collections are too frequent.

For those with concerns over budgetary requirements it is worth bearing in mind that a single location 'average office-based' business with up to 85 employees would expect to pay £585 per year for a secure

shredding service. Approximately £45 per collection (one collection every four weeks), a small price to pay for complete peace of mind.

About Russell Richardson

Russell Richardson delivers secure commercial destruction services that ensure full compliance with the Data Protection Act and protection against corporate identity theft. From a secure depot in Sheffield, the team provides total commercial waste and recycling management via on-site mobile and off-site confidential document shredding, data, media, uniform and product destruction, as well as WEEE compliant computer equipment recycling and disposal. A founding member of the National Association for Information Destruction (NAID) Europe, Russell Richardson adheres to the strict security standards set in BS EN15713:2009, the European standard for the destruction of confidential information and operates to ISO9001:2008.

A family-run business operating for over 33 years, Russell Richardson is both flexible and efficient in its approach to customer service. Reacting quickly to new customer requirements, it can adapt any service lines to effectively integrate with any business large or small.

For more information visit: www.russellrichardson.co.uk or call 0800 294 6552.