

## Playing it Safe: Document Destruction Best Practices

Organizations that possess important confidential information about their own operations or about their customers may become a target for identity theft and fraud, with dire consequences in terms of reputation and cost. According to Ernst & Young's 2008 Global Information Security Survey, senior executives from different countries believe **a security incident would have an even greater impact on reputation and brand than on revenue**. Eighty five per cent cited damage to reputation and brand as significant, compared to 72 per cent for loss of revenue and 68 per cent for regulatory sanctions.<sup>1</sup>

*"Accessibility to documents that contain confidential data poses a serious threat to*

*the business and reputational integrity of any organization,"* says Michael Skidmore, Chief Security Officer at Shred-it. *"It's only common sense that organizations should do what it takes to prevent any compromises of their information, identify security loopholes and implement effective and reliable measures to address them."*

Secure document destruction is one of such measures. Based on its 20-plus years of experience in this business, Shred-it shares some tricks of the trade and practical tips on how to make sure your confidential information stays confidential.

*Welcome to the third issue of Securing the Future, a newsletter from Shred-it document destruction. Focusing on the issues of information security, privacy and compliance, this newsletter shows how these issues affect your organization and your customers and, most importantly, how you can best address them.*



### Secure document destruction at a glance

Best practices in document destruction can be summed up as three general guidelines that are easy to understand and implement:

**01 Shred it all on a regular basis** and avoid the risks of human error or poor judgment about what needs to be shredded. Deter the accumulation of confidential paper waste that is stored in different parts of your office, creating a security risk.

**02 Shred before recycling** and spare yourself from worrying about what happens to your confidential paper waste once it is at the recycler or in transit to the recycler.

**03 Shred using a professional service** and ensure there are no security loopholes anywhere in the process. Outsourcing also saves the time and resources of your employees.

When implemented in a strategic and integrated way, these principles will dramatically increase the security of your documents, your business and your customers. But let's look at them one at a time.



# 01

## Best Practice: Shred it all on a regular basis

A “shred-all” policy is one of the most critical steps you can take towards total information security. It means a department or company-wide commitment to shredding all documents on a regular basis. Standardizing document destruction procedures will allow your organization to align its rules and regulations with its information security goals and needs.

A shred-all policy is a way to make sure there are no leaks – intentional or unintentional – of your organization’s sensitive information to outside sources. This may potentially include criminal groups that feed on this sensitive information to commit fraud and identity theft crimes. In turn, regular disposal of paper waste means it does not accumulate in a chaotic manner, reducing the potential for security breaches resulting from negligence or malicious intent.



Regular information security audits will help you identify areas of vulnerability and potential risks. Some security audit best practices include:

- Conducting audits on a regular basis.
- Updating your document destruction policies accordingly based on your audit findings.
- Ensuring your employees are in compliance with your audit policies, as well as identity theft and privacy legislation.

- Training your staff in secure document destruction procedures. Show them your commitment to the cause and help them understand the importance of protecting your company’s – and your customers’ – confidential information.

Full cooperation of your employees is paramount, but a word of caution is in order. While most security threats may be perceived to be outside of your organization, don’t overlook the potential for internal threats. Your staff may actually be one of them. According to the US-based Healthcare Information and Management Systems Society, up to 23 per cent of all breaches that required notification since 2000 have been caused by an employee.<sup>3</sup> Important information can be lost, stolen or mishandled by your staff members. That’s why limiting the number of people who have access to confidential data and enforcing security guidelines on all levels of an organization is so important.

# 02

## Best Practice: Shred before recycling

You may think you are doing your part for the environment by tossing paper into the recycling bin. However, are you recycling in a security-conscious manner?

Remember: loose paper is often unattended before it has been recycled, and it can leave your organization vulnerable to potential security breaches. For example, unguarded paper in recycling containers can be misplaced or stolen. Or, it can simply fall out of the recycling truck and onto the street.

There is a way to meet both needs – serving the environment and practicing responsible business by recycling



documents while also keeping your customers’ confidential information confidential. You can achieve both goals by outsourcing document destruction to

a reliable document destruction service provider with high security standards and a strong environmental record.

You might find it interesting to know that, working with Shred-it, organizations save one tree through recycling every time they fill up two Shred-it security containers with paper. Shred-it even offers customers an annual Environmental Certificate, which states how many trees they have saved. What’s more, by using recyclable, biodegradable, hydraulic fuels for its vehicles, Shred-it proves its commitment to continuing to improve its environmental practices.

## Best Practice: Shred with a reliable supplier

By implementing all these measures, you'll come a long way toward the ultimate goal – total security of your business and customer information. However, one question remains - should you hire a third party provider or try pursuing these measures on your own? Here are a few pointers to help you ponder this question:

- When you outsource document destruction, you **free up your staff to concentrate on what matters the most** – your business and the bottom line. This means productivity savings of up to 15 - 20 per cent, according to Shred-it's analysis of the number of employees generating and shredding paper, the time it takes them and their hourly wage.
- This estimate does not reflect the potential costs of litigation, expensive fines, reputation damage, loss of trust and negative media coverage potentially caused by security breaches, resulting from insecure document destruction practices. According to Forrester Research Inc., companies that experienced security breaches in the U.S. in 2006 lost between \$1 million and \$22 million.<sup>iii</sup> In Canada,



identity theft may cost businesses and consumers approximately \$2.5 billion, according to the Canadian Council of Better Business Bureaus.<sup>iv</sup> And in the U.K., businesses can suffer between £30,000 to £250,000 from security-related reputation damage alone.<sup>v</sup> Professional document destruction by a reliable third-party provider will help make sure such breaches do not happen.

- **Most organizations do not have the expertise to ensure total security** of the document destruction process, nor do they have the equipment necessary for storing and shredding sensitive documents, such as locked security consoles and powerful shredding machines. Finally, they do not have the human resources needed to support the tight chain of custody around the document destruction process.

Shred-it's on-site locked document storage containers ensure that once documents are ready to be discarded, they remain secure and protected until Shred-it personnel arrive. Those documents are then securely moved to a Shred-it truck, following a tight chain of custody. There, on your premises, they are fully destroyed, leaving only small confetti-like pieces of paper. Shred-it completes the process, issuing a Certificate of Destruction to provide verification that documents have been securely destroyed.

By outsourcing your document destruction needs, you gain access to the years of experience and deep expertise of a professional document destruction service provider. In doing so, you significantly reduce the risk of unfortunate missteps or accidents, potentially leading to security breaches, privacy violations, identity theft and fraud.

- (i) Ernst & Young's 2008 Global Information Security Survey, [http://www.ey.com/Global/assets.nsf/Canada/GISS/\\$file/GISS2008.pdf](http://www.ey.com/Global/assets.nsf/Canada/GISS/$file/GISS2008.pdf).
- (ii) Hospitals often fail to notify patients of data breaches; Regulatory loopholes keep patients in the dark, report says, Jon Brodtkin, 11 April 2008, [www.networkworld.com](http://www.networkworld.com).
- (iii) Forrester Research Inc.
- (iv) Canadian Council of Better Business Bureaus.
- (v) Information Security Breaches Survey 2008, The Department for Business, Enterprise & Regulatory Reform (BERR).



Making sure  
it's secure.™

Shred-it is a world leading information security company providing services that ensure the security and integrity of our customers' private information. The company operates 140 service locations in 16 countries worldwide, servicing over 150,000 global, national and local businesses, including the world's top intelligence and security agencies and more than 500 police forces, 1,500 hospitals, 8,500 bank branches and 1,200 universities and colleges.