

FINANCIAL INSTITUTIONS LEADING THE WAY IN INFORMATION SECURITY PRACTICES

You have heard the shocking statistics about identity theft and you know enough to destroy or secure your personal information. But what about the information your organization collects about its customers? Can your customers trust your organization to look after their personal information as well as you look after your personal information?

One industry that collects and stores a lot of valuable information about all of us is the financial services industry – our bank, insurance company, credit union or accountant. However, you may find it a relief to know that, based on studies, financial institutions overall experience less security breaches than other industries.

“When it comes to customer security, banks and other financial institutions are often at the forefront of positive change, and this is hardly a surprise, given the amount of sensitive financial and personal information that flows through their databases and files,” says Vincent De Palma, CEO of Shred-it. “By implementing a number of business processes and customer education programs to ward off identity theft and fraud, banks have achieved a great deal already, but the process of learning and improving should never stop.”

The focus of this whitepaper will be on professionally-managed document destruction as a critical component of information security in the financial services context.

SECURITY GAP ANALYSIS IS THE FIRST STEP

In 2007, a massive TJX/Winners security breach jeopardized 45.7 million credit and debit cards. Such breaches expose massive amounts of sensitive customer information, creating the pre-conditions for identity theft and fraud, and potentially resulting in loss of customer business, legal actions and costly fines. The reputational and brand damage that can come as a result of exposing this information cannot be discarded either. According to the Ponemon Institute, in 2008, the average cost per compromised customer record to a company in the U.S. was \$202, while the average total cost per data breach amounted to \$6.65 million.

Because of these risks, in the countries with advanced information economies, such as the US, Canada and the UK, most large financial institutions do their due diligence to protect their information both in electronic and in paper form. While the security of electronic systems is usually a clear area of priority, paper document security is often discounted. Companies can assess how well they are doing in this respect, using a checklist below from Shred-it, which guides company decision-makers through the analysis of possible security gaps in their paper management process. When looking at your paper waste, they should ask the following questions:

- Which paper documents are selected to be destroyed? Who makes this selection? Is there a company document destruction policy?
- Is all paper waste fully destroyed?
- Is it destroyed on a regular basis? (ideally, it should be destroyed at least once every week)
- How and where is it destroyed? Where are paper documents stored before being shredded? Are there any security loopholes along the way, such as depositing some or all paper waste in unprotected recycling totes or ordinary garbage bins?
- Is the same document management and destruction process consistently implemented throughout your organization?
- Are staff in each department trained on proper document destruction processes?
- Are there formal information security policies in place, covering secure document destruction and employee access to sensitive information? When were they written or last reviewed?
- What are the organization's overall attitudes and culture around managing the paper trail?

Some typical security loopholes include:

- Disposing of documents in ordinary garbage bins or recycling totes.
- The use of similar-looking totes for confidential and non-confidential paper waste, which may be easily mixed up or used with no differentiation by the employees.
- Disposing of documents in garbage bags left outside of the building for pick-up by garbage collection services.
- Disposing of documents in recycling bins, without prior shredding.
- Employee negligence or wrongdoing:
 - Unauthorized access to confidential information.
 - Abandoning, leaving unsupervised, losing, stealing or sharing confidential data with unauthorized parties – typically in paper form, on laptops or on other portable storage devices.

ADDRESS SECURITY, COSTS, PRODUCTIVITY AND COMPLIANCE

Managers in the financial services industry, similar to other organizations, face a series of decisions they need to make with regard to document management and disposal. Maintaining compliance may be their first consideration.

In the US, banks are subject to the Fair and Accurate Credit Transactions Act (FACTA), the Gramm-Leach-Bliley Act, which protects the privacy of consumer information held by financial institutions, as well as the Sarbanes-Oxley Act (SOX), regulating financial reporting.

In Canada, in addition to the Bank Act which regulates the country's chartered banks, banks are subject to the Personal Information Protection and Electronic Documents Act (PIPEDA). Overseen by the Privacy Commissioner of Canada, PIPEDA places the onus on Canadian private organizations, including banks and other financial institutions, to protect the personal information of its customers.

In the UK, the financial services industry is regulated by the Financial Services Authority (FSA), setting strict rules with regard to data security, with the maximum fine for a data breach exceeding £5 million.

Chris Eldridge, Head of Group Office and Facilities Management Services at the financial services group Brewin Dolphin in the UK, says that part of their security strategy is a shred-all policy. Brewin Dolphin employs around 1,700 staff in the UK, the Channel Islands and Ireland, across a network of 40 sites. Among its services, the company offers investment banking, and a number of its staff handle price-sensitive and other confidential information. Brewin Dolphin considers all printed matter to be confidential, including handwritten materials and even the newspapers, where employees may write notes.

While most large financial services organizations work with one or several third-party document destruction providers, some still shred their paper waste in-house. "In some cases, in-house document destruction is justified," says Andrew Lenardon, Manager, US Major Accounts Sales at Shred-it. "But a more common story is when the advantages of outsourced document destruction outweigh in-house shredding for a number of reasons, ranging from information security to staff productivity."

Based on such variables as the number of employees generating and shredding paper, the time it takes them to shred and their hourly wage, Shred-it experts calculated that outsourced document destruction, compared to in-house, creates productivity savings of approximately 17 per cent.

Mr. Eldridge of Brewin Dolphin acknowledges that before signing their current document destruction contract with Shred-it, the company shredded its documents in-house. In many cases, staff had to work overtime to keep on top of their shredding obligations. A special challenge for Brewin Dolphin was the vulnerability of its data to potential wrongdoing from third-party suppliers. Cleaning staff, for example, had access to more office areas than regular staff members – a particularly serious issue for multi-site companies, such as Brewin Dolphin, which has grown through acquisition and expanded its range of suppliers.

Based on the amount of employee overtime spent on shredding, as well as the quality of in-house shredding and security considerations, the company's team made a case that hiring a third party would be beneficial in terms of costs, security and efficiency. Currently, all Brewin Dolphin offices are equipped with Shred-it locked security containers, where their confidential waste is stored until the containers are opened by Shred-it staff. A Brewin Dolphin staff member accompanies the Shred-it employee around the building, waits while the documents are shredded in a Shred-it truck and then does a final check to ensure that all documents have been destroyed securely.

"Not all organizations choose such close supervision of different stages of our document destruction process by their employees," says Robert Guice, Senior Vice President EMEA. "However, we encourage full transparency when it comes to the integrity of our service and chain-of-custody procedures"

SMALL BUSINESSES STILL TO CATCH UP

While you may expect large financial institutions to have far more stringent document destruction security policies in place than smaller organizations, the protection of customer data is still of the highest importance. Many smaller financial institutions pride themselves on following the same stringent practices that are set by the larger companies, and many rely on the same third party providers to ensure they are also compliant with privacy laws.

One of these companies is Cerefice & Company in Rahway, New Jersey. Tom Corley is president of the company which provides tax, accounting, estate, financial planning and

other financial services. When Mr. Corley took over the firm in 2003, he was surprised to discover all paper waste went to regular garbage boxes and was left unshredded outside of the building for pick-up by municipal garbage-collection services.

“It was common sense that (those practices) needed to change,” says Mr. Corley. “Anything could happen with these documents outside. They could be blown away by the wind, or someone could take them.”

Exploring other options, Mr. Corley looked into the possibility of purchasing a high-power shredding machine and assigning someone on his team to shred paper waste on a regular basis. However, he ultimately decided to hire a professional document destruction company recommended by a colleague. Now working with Shred-it, Cerefice & Company has a “shred everything” policy. Examples of documents deposited for destruction include tax return printouts, financial statements, credit card statements, banking records and other financial information.

During the busy tax season, Cerefice & Company has the contents of the containers shredded twice a week, and, at other times, twice a month. “Working with Shred-it, we minimize the risks (of fraudsters) who look to steal Social Security Numbers and other personal information, gaining our customers’ personal data,” says Mr. Corley. While he sees increased security as the primary benefit of the professionally-managed shredding process, he also acknowledges the “incremental savings associated with reducing human resource cost,” adding that by having its document destruction needs handled by Shred-it saves his employees time “so they can focus on what they do best.”

BEST PRACTICES: HOW TO MAKE DOCUMENT DESTRUCTION SECURE

Document destruction best practices can be summed up as four principles that are easy to understand:

- Shred all – to avoid the risks of human error or poor judgement
- Shred regularly – to deter the accumulation of confidential paper waste
- Shred securely– to ensure the chain of custody meets your compliance requirements
- Shred before recycling – to avoid risks of once confidential paper waste is at the recycler

When implemented as a process, these tenets dramatically increase the level of document security, reducing the potential for human error and create a tight chain of custody around the entire document destruction process. “Each and every single day, employees should deposit all of their paper waste that they collect throughout the day in locked containers, where it is stored until professional, security-cleared and specially-trained staff destroy it completely before recycling,” says Mr. Lenardon from Shred-it.

It is important to remember that while recycling paper is an excellent way to enhance environmental sustainability, recycling should only be done after shredding.

Another consideration is that not all shredding methodologies provide the same level of security. For example, strip shredding does not guarantee full security protection because, with some effort, paper pieces can be matched together to restore a confidential document. Only cross-cut methodology, which reduces paper waste into unidentifiably small confetti, guarantees a high enough level of security.

Other best practices that financial institutions use to ensure the safeguarding of confidential information include:

- The use of special equipment, such as locked paper waste containers and powerful shredding machines, that can, in a fast manner, destroy large volumes of office waste.
- The possibility of viewing the full document destruction process through a security screen.
- The receipt of documents by the shredding company certifying that paper waste has been securely destroyed.
- Ensuring a tight chain of custody, bypassing any storage and/or unnecessary shipping of confidential information that might create potential security loopholes.

THE SHRED-IT SOLUTION

Shred-it, the world's leading information security company, draws its best practices from its extensive experience serving approximately 8,500 customers in the financial services industry. "The operational environment of banks, credit card providers, insurance companies, investment funds and other financial services organizations continues to increase in complexity," says the company's CEO, Vincent De Palma. "We understand this environment and we know how to bring value that extends beyond the physical destruction of waste paper."

"We see ourselves as a strategic partner with the financial institutions which contributes value in different ways," continues Mr. De Palma. "One of the ways we provide value is by helping organizations identify potential security risks. Another way we provide value is by providing the services to manage them proactively." By developing document destruction solutions for individual financial services clients, Shred-it not only helps organizations address their unique security needs, but also takes care of their document destruction needs so they can focus on their core business goals.

In summary, Shred-it's value includes:

- Developing document destruction solutions that are high-value and cost-efficient.
- Implementing proven document destruction best practices.
- Having pre-screened, bondable customer service representatives.
- Ensuring full chain of custody and other procedures around managing confidential documents that significantly minimize the potential for human error and provide the highest level of security.
- Inviting company personnel to view the document destruction process.
- Providing a "Certificate of Destruction" upon completion of the document destruction process.
- Providing a certificate of environmental accomplishment, recognizing and quantifying a company's positive environmental impact by having its waste paper recycled.
- Being able to provide on-site or off-site service to match your compliance requirements from all locations so you don't have to manage multiple vendors.

As the risks of identity theft and fraud in the financial services industry continue to increase, mitigating these risks has become extremely important. In addition, organizations that are found at fault of losing their customer information can suffer fines, charges and loss of reputation and customers. Using a professionally-managed and secure document destruction process, companies can achieve the peace of mind needed to focus on their business.

About Shred-it

Shred-it is a world leading information security company providing services that ensures the security and integrity of our customers' private information. The company operates 140 branches 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 8,500 bank branches, 500 police forces, 1,500 hospitals and 1,200 universities and colleges.

Shred-it contact information:

T: 905-829-2794

F: 905-829-1999

Website: www.shredit.com