

# SECURE DOCUMENT DESTRUCTION PROCESSES CRITICAL TO BUSINESS SUCCESS

## THE CASE FOR OUTSOURCING DOCUMENT DESTRUCTION TO INCREASE SECURITY AND DECREASE COSTS

### INTRODUCTION

Information security breaches, often leading to privacy violations, identity theft and fraud, are on the rise. A truly international problem, this issue knows no borders and affects individuals and organizations alike. While the full consequences are hard to measure, one thing is clear – the costs of compromised security are high.

According to the Ponemon Institute, in 2008, the average total cost of a data breach in the U.S. was \$6.65 million, up from \$6.35 million in 2007 and \$4.54 million in 2005. Canada's Justice Minister Robert Nicholson estimated that identity theft may cost Canadians more than \$2 billion a year, as reported by Canada's CTV. In the UK, this number is close to £1.2bn a year, or £25 per person, according to the UK's Home Office Identity Fraud Steering Committee.

How can various stakeholders – from consumers to businesses to hospitals to government agencies and beyond – minimize the risks of confidential data falling into the wrong hands? While there are many possible solutions, this paper will focus on one solution - making a case for secure outsourced document destruction a critical part of any organization's information security strategy.

### SECURITY RISKS

Today, our personal information is fed into multiple databases that belong to banks, medical institutions, pharmacies, government agencies, law and accounting firms and a great number of other organizations. These databases are increasingly digitized. Hospitals in the US, Canada and the UK are undergoing the transition to electronic medical records. Governments encourage citizens to file their taxes and apply for passports online. Business companies assemble detailed consumer profiles, refining their marketing prowess. This sensitive and often confidential customer information is channeled to complex databases, often consolidated online and shared with other organizations.

Undoubtedly, the convenience of having this wealth of information at one's fingertips anytime and anywhere, for business, medical, research and many other purposes, is enormous. But the risks of this information being used fraudulently or simply mishandled are significant, too.

While the electronic management of confidential data – particularly online – creates a number of challenges, many breaches can still be traced back to mishandled, lost or stolen paper documents. Organizations that deal with customer information, such as family doctors' offices, accounting or law firms, continue to receive and store much of this customer information in paper-based form. Regardless of their extent of digitization,

most companies, government agencies and other entities are still producing large volumes of paper documents leading to ongoing challenges of managing confidential information.

Even when customer records are maintained electronically, there are numerous occasions when they are printed out and circulated, in paper form, within and, sometimes, outside of the organization. Loosely managed paper documents may become the vehicle of security breaches. Here are a few general examples taken from the recent media:

- Personal information, including patient names, social security and social insurance numbers, addresses and personal medical information found, in recycling bins or dumpsters outside of medical offices or in dumpsters
- Boxes of customer receipts and patient records being stored in unsecure or unsafe locations that can be easily accessed
- Documents from businesses placed in garbage or recycling bins
- Human error resulting in business documents being misplaced, dropped or lost

While some security breaches have been widely publicized in the media, there may be many others that have not warranted the media's attention.

## **FACTS AND FIGURES**

The costs of security breaches may involve a range of negative consequences, from financial and legal to reputational, psychological and even medical, and these costs tend to be high for businesses and individuals alike.

### **Costs to businesses**

- In Ernst & Young's 2008 Global Information Security Survey, it was found that senior executives from different countries believe a security incident would have a greater impact on reputation and brand than on revenues. Eighty-five per cent of them cited damage to reputation and brand as significant, compared to 72 per cent for loss of revenues and 68 per cent for regulatory sanctions.
- According to a research study conducted by the Ponemon Institute and sponsored by PGP Corporation, in the US, the highest impact associated with a data breach is the cost of lost business. This cost averaged \$4.9 million or \$139 per record compromised. Lost business now accounts for 69 per cent of data breach costs, up from 65 per cent in 2007, compared to 54 per cent in the 2006 study.
- According to Forrester Research Inc., in the US in 2006, companies that experienced security breaches lost between \$1 and \$22 million.
- Recent research from the Department for Business, Enterprise & Regulatory Reform (BERR) reveals that the average total cost of a UK company's worst security breach can be between £10,000 and £20,000, with associated costs increasing with the size of the company. For large businesses (more than 250 staff), it is between £90,000 and £170,000, and for very large businesses (more than 500 staff), security breaches can cost between £1 million and £2 million. When incidents become known about externally, the survey revealed damage to reputation could cost large businesses between £30,000 and £250,000.
- According to the Canadian Council of Better Business Bureaus, identity theft costs Canadian consumers and businesses an estimated \$2.5 billion dollars a year.

- IDC Canada estimates that more than half of the overall cost of a privacy breach per record can be attributed to "customer opportunity costs," comprised of brand damage, loss of existing customers and difficulties of attracting new customers.
- A Rotman-Telus Joint Study on Canadian IT security practices provided the following breakdown of annual losses associated with security breaches:
  - Government organizations lose an average of \$320,000;
  - Private companies lose \$294,000; and
  - Publicly traded firms lose approximately \$637,000.
- Sixty-five per cent of the respondents in the Rotman-Telus Joint Study survey said their organization's privacy policies are enforced to an acceptable degree, but only fifty-four per cent made the same claim about their security strategies.

### **Costs to consumers**

- The US Federal Trade Commission estimates that as many as nine million Americans have their identities stolen each year, while the US Department of Education notes that identity theft is one of the fastest growing crimes in the US, costing victims over \$5 billion annually.
- According to a 2008 survey of Canadian consumers conducted by McMaster University's eBusiness Research group, 6.5 per cent of Canadian adults, or almost 1.7 million people, fell victim to identity fraud in 2007. These victims spent over 20 million hours and more than \$150 million to resolve problems associated with these frauds.
- As noted previously, this number is close to £1.2bn a year, or £25 per person, according to the UK's Home Office Identity Fraud Steering Committee.

### **BUSINESS SOLUTIONS TO SECURITY RISKS**

Some of the highest impact cases of security breaches, with potential to trigger multiple cases of individual identity theft and fraud, originate inside organizations. For example, when millions of customers of a large North American retail organization had their credit card information stolen, their only recourse was to monitor their own cards for suspicious transactions.

It is the responsibility of businesses to take proper care of their customers by implementing effective security strategies. Typical solution components include:

- Correctly identify an organization's unique security vulnerabilities and risks and have ongoing risk analysis in place.
- Have a strategic approach to managing information security, targeting both electronic and paper-based sources at all stages of the information cycle, from data generation to storage and transfer to document destruction.
- Have stringent policies regulating insider access to sensitive information and limit the number of people who handle confidential documents.
- Have sufficient funding for effective security systems. In difficult economic times, forward-looking companies tend to increase their investment in information security. According to Ernst & Young's 2008 Global Information Security Survey, despite tightening economies worldwide, 50 per cent of companies are set to increase their information security budgets.

Customers can help themselves by ensuring the businesses that they deal with have the proper processes in place to safely and securely manage their personal information. If the business does not seem to have processes in place to keep information secure,

customers should be wary of providing them with personal information. In addition, they should collect and destroy all receipts and other sensitive documents, as needed.

### **SECURE DOCUMENT DESTRUCTION – A CRITICAL COMPONENT OF THE SECURITY STRATEGY**

Secure document destruction is a critical part of a business' overall information security protection process. Today, many businesses use some form of document shredding service and most large companies outsource their document destruction functions. However, shredding methodologies and the degree of compliance vary widely from vendor to vendor. Security gaps in the process that organizations and their providers use to store and dispose of paper waste may create conditions that make paper documents easy to mishandle.

Unfortunately, employees can be the weakest link in this process. In fact, employee negligence or wrongdoing is among the most common causes of security breaches. In addition to misplacing paper files, company insiders who have access to sensitive customer information may use it for fraudulent purposes, sometimes collaborating with criminal groups and selling the information. In the US for example, where approximately 50 million people are uninsured for health care coverage, health care system employees might sell medical information to criminals for \$5 to \$50 a name, according to the Chicago Tribune. Potential security loopholes in any business environment, including health care, may include:

- An accessible and unsupervised file room;
- Document folders left unattended on staff desks;
- Unsecured recycling bins;
- Untrained staff (in terms of confidential information handling); and,
- Absence of document destruction processes and services.

### **DOCUMENT DESTRUCTION BEST PRACTICES**

To minimize the risks of confidential information being used fraudulently or mishandled, proactive companies tend to follow a number of document destruction best practices, including:

- Ensure document destruction services are part of an enterprise-wide systemic strategy, addressing not only security issues, but also compliance, financial, productivity and environmental considerations.
- Align document destruction processes with national and provincial legislative and regulatory requirements. (For more information on legislation affecting security and privacy, please visit: <http://www.shredit.com/resources.asp>.)
- Support a "shred-all" policy, where all waste paper is fully destroyed on a regular basis.
- Work with reliable third-party partners who assure total security, address the business' unique needs and offer consistent, standardized document destruction services nationally or even internationally.
- Introduce and consistently implement company-wide document destruction policies; including employee training.
- Choose environmentally sustainable document destruction practices.
- Outsource document destruction to professional security providers; leverage their expertise, methodology and special equipment, such as locked shredding consoles

and powerful shredding machines that can destroy large volumes of paper waste quickly.

### **SECURE DOCUMENT DESTRUCTION AS A BUSINESS IMPERATIVE**

The benefits of secure document destruction, while not always obvious, should not slip under the radar of organizational decision-makers. By investing in a secure document disposal process, they invest in the security of their and their customers' information, and in their business' reputation and long-term success.

- Companies using secure document destruction may also avoid paying the hard-to-quantify hidden costs of litigation and negative media attention associated with security breaches.
- According to Socratic Technologies, 74 per cent of document destruction clients destroy documents to protect the privacy of their clients; 68 per cent do it to prevent identity theft.
- According to Shred-it's research, businesses can save 15 to 20 per cent by hiring an outside document destruction service provider. The research included calculations on the amount of paper generated, the hourly wages of staff assigned to document shredding and the time paper shredding takes when using an in-house shredder. There is also the missed opportunity cost of doing in-house shredding, as it is likely staff could be doing more productive work than shredding paper. Therefore, by using an outsourced document destruction provider, companies can create significant productivity gains.

### **CONCLUSION**

The issue of secure document destruction is an issue that all businesses should discuss. With the ongoing digitization of information, the risks of security breaches – as well as identity theft and fraud – will increase, while electronic and paper-based information sources will continue to be closely intertwined. The pace of technological progress cannot be stopped, but organizations can and must take responsibility for protecting the security of the customers they serve. Secure document destruction is a vital part of the security process.

### **ABOUT SHRED-IT:**

Shred-it is a world-leading document destruction company providing compliant services that ensures the security and integrity of 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 500 police forces, 1,500 hospitals, 8,500 bank branches and 1,200 universities and colleges. For more information please visit [www.shredit.com](http://www.shredit.com) or call 1.877.60 Shred.