

# SECURING THE FUTURE

## In this Issue

- Reputation: your most valuable and fragile business asset
- The risks to your company's reputation
- Shred-it's tips for reputation protection and security breach prevention
- Your free security consultation



Don't Throw  
Your Reputation  
in the Waste Bin

Have you really pondered the impact of a security breach? It can lead to regulatory fines, identity theft and fraud, unhappy clients or employees, negative media attention and expensive lawsuits. Additionally, your organisation's intellectual property and commercial secrets could be leaked to your competitors. As you can see, the damage of compromised security can be significant, and potentially devastating, to any organisation's reputation and brand.

## Reputation: your most valuable and fragile business asset

In recent uncertain economic times, the pressures to cut costs have been immense. It is important, however, not to lose sight of your organisation's long-term goals and most valuable business assets. Reputation is one of those assets — powerful, yet intangible and fragile, it serves as the hallmark of your company, attracting resources and business and supporting long-term profitability.

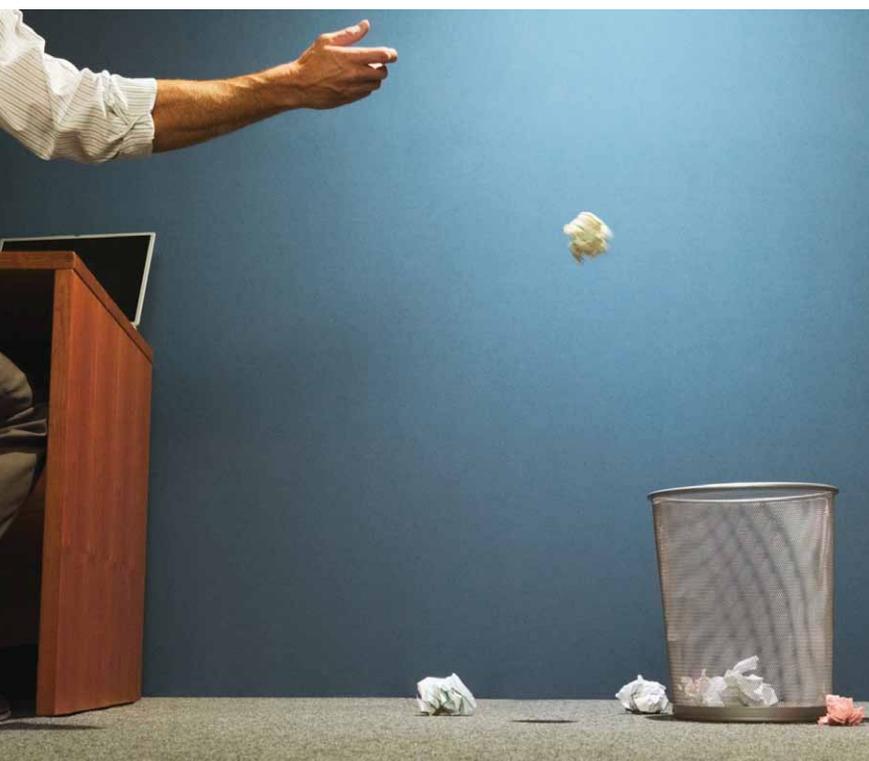
In an ever more connected world where users' experience of products and services — both positive and negative — can be shared more widely, quicker and with more people than ever before, the value of a good reputation (and, conversely, the damage caused by a bad one) is surely only going to increase. If your products and services are meeting your customer's needs, reputation is the engine that will continue to drive growth, increase profits and help you beat the competition.



# SECURING THE FUTURE

Reputation is defined by more than your company's services and products. Vincent De Palma, President and CEO at Shred-it says, "Leading companies understand that serving their clients also means protecting them, particularly from any harm caused through these companies' own actions." De Palma continues, "In this digital age, one of the most important individual rights is the right to privacy, which is closely related to the security of our personal information. New and existing laws and regulations recognise and protect these rights, and so should all businesses and organisations, large or small. Furthermore, this protection should extend beyond your clients to your business partners, employees and all stakeholders."

The protection of this sensitive information is critical to an organisation's ability to conduct business with various stakeholders. If your clients or partners have concerns about the security of their financial or personal information while it's in your care, they may take their business elsewhere. This loss of business is almost a certainty if the security of their personal information has been compromised while in your custody. Conversely, an untarnished reputation will give your customers, employees and partners the level of comfort they need to count on you as a trusted partner.



To further quantify the cost of a data breach, it has been estimated that security breaches in the UK cost over £2.2 million per incident — that's according to the 2014 Cost of Data Breach Study for the UK conducted by the Ponemon Institute.<sup>1</sup> What's more, lost business costs — including abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill — account for £950,000 of that total.

Given these far-reaching consequences and ever-increasing expenses, you're likely to be asking yourself, "How can I protect my company and its brand integrity from a security breach?" We'll tackle this question next as we move through this newsletter.

<sup>1</sup> Ponemon Institute/IBM, 2014 Cost of Data Breach Study: United Kingdom, [www.ponemon.org](http://www.ponemon.org)



# SECURING THE FUTURE

## The risks to your company's reputation

What factors jeopardise your organisation's reputation? You'd be surprised at the daily tasks and potential risks associated with everyday work activities that can place your confidential information, and your company, at risk:

- Confidential information thrown away in waste or recycling bins. Third-party services (such as cleaning or maintenance contractors) have access to your premises and potentially unsecured documents or devices.
- Emails or internal communications containing confidential information are mishandled or lost.
- Unsecured networks can be easily hacked.
- Malicious or disgruntled employees may intentionally steal information.
- Lost portable devices such as laptops, smart phones or USB drives.
- Hard drives — including those from digital photocopiers — containing confidential information aren't correctly destroyed.

Electronic breaches receive the bulk of media coverage, yet "low-tech" security breaches involving paper documents account for a significant proportion of incidents deemed serious enough for the Information Commissioner's Office (ICO) to impose a monetary penalty on the organisation at fault. These breaches included sensitive documents: being left in filing cabinets that were then sold to the general public; left behind after premises were vacated; left on a train; ending up in a supermarket car park recycling bin; and faxes being sent to the wrong recipients.<sup>2</sup>

The most common threats occur when documents containing confidential information are recycled or thrown away without being destroyed. Small and medium-sized businesses are especially vulnerable to such risks. Due to their size and their focus on growth, they may not have formal information security policies and procedures in place. According to Shred-it's 2014 Information Security Tracker survey only just over half (54 per cent) of SMEs said they had a protocol that was strictly adhered to by all employees.<sup>3</sup>

Companies of any size should realise that taking risks with the security of their customer and business information could lead to potential repercussions such as: litigation costs, fines, negative media attention and reputation damage. A secure document destruction process allows organisations to not only invest in their security and reputation, but also in long-term productivity.

<sup>2</sup> ICO, Monetary Penalty Notices, [www.ico.org.uk](http://www.ico.org.uk)

<sup>3</sup> Ponemon Institute/IBM, 2014 Cost of Data Breach Study: United Kingdom, [www.ponemon.org](http://www.ponemon.org)



# SECURING THE FUTURE

## Shred-it's tips for reputation protection and security breach prevention

The damage that a security breach can do to your organisation's reputation can be expensive, long-lasting and even catastrophic. Our focus now turns to prevention and steps you can take to reduce your security risk:



- Adopt a “shred all” policy. A simple and effective way to improve your information security is to shred all documents, regardless of content.
- Shred before recycling. Shred confidential documents before recycling — don't let them sit unattended in recycling bins or be intercepted in transit once they leave your office.
- Limit insider access. You can prevent insider information theft by limiting internal access to confidential information.
- Train your staff. Make security a top priority by training every employee about what constitutes confidential information and how to dispose of it.
- Ensure your security policies keep pace with trends in technology by creating measures that protect your organisation when employees are working away from the office.
- Create a culture of security — a good first step is to implement an information security policy. Educate all employees and conduct regular security audits of your office to assess its security performance.

For more information on how to avoid data breaches and implement proper document destruction best practices in your business, visit Shred-it's [online resource centre](#).

## Your FREE security consultation

To conduct your own information security self-assessment, Shred-it has developed an online survey to help businesses better understand security gaps. You can access it via the following link: [shredit.co.uk/information-security-best-practices-and-checklist](https://shredit.co.uk/information-security-best-practices-and-checklist)

You can also visit Shred-it on [Facebook](#) and [LinkedIn](#) or follow us on [Twitter @Shredit\\_UK](#).

