SECURING THE FUTURE

Shred-it

Secure Document Management & Destruction as Part of Crisis Planning

In May this year the Information Commissioner's Office, the independent body responsible for protecting the data privacy of individuals, reported that the number of complaints it has received regarding data breaches had reached 1,000.

This highlights that many organisations are failing to address the issue of data security. A number are yet to put in place adequate guidelines on securing confidential information and still do not view the destruction of both paper and electronic documents as an essential part of information security.

Robert Guice says: "When sensitive documents, such as legal files, medical records or even employees' personal data are left unsecured they are at risk of being misplaced, misused or stolen and this can lead to serious long-term financial, legal and reputational issues. The risk of this happening during a disruption becomes far greater as fraudsters take the opportunity to enter a deserted workplace and walk away with documents containing confidential information about your organisation, your associates, your employees and your clients."

It is essential that there is a strategic and systemic effort to address information security at all levels to prevent document management and destruction from being left to chance or to the discretion of individual managers or employees.

Documents that are partially destroyed, for example in a fire or a flood, can lead to a data breach and while there is no single recipe for success, information security measures that are applicable to most organisations include:

- Restricted or differentiated levels of access to sensitive records
- Secure storage of printed documents in locked cabinets
- Disposing of office paper waste in special security consoles
- Regular onsite document destruction using cross-cut methodology that transforms paper documents into unidentifiably small pieces
- Consistent information security policies, whose implementation is supported by a senior team committed to data security and the adoption of a security conscious culture throughout the organisations

Implementing these measures ensures that there are no confidential documents left unattended in your office because they are either filed away securely or have been completely destroyed. Should a crisis hit, the risk of an information security breach is dramatically reduced, regardless of what happens with the rest of your organisation's waste.

Welcome to the seventh edition of Securing the Future, a periodic e-newsletter from Shred-it. In this issue we are looking at how disruptions both inside and outside of the workplace can leave organisations vulnerable to a data security breach if inadequate document security measures are in place.

While the likelihood of your organisation being flooded or going up in flames is extremely low, the cost to organisations can be high and can be higher still if such an event leaves you exposed to a breach of confidential information.

With the Information Commissioner's Office (ICO) now able to fine organisations up to £500,000 for serious data breaches of the Data Protection Act, it is more important than ever that organisations do everything they can to ensure that confidential data is secure or else run the risk of severe financial loss together with the reputational damage associated with a public fine.

It is important to note that it can be difficult to implement adequate security measures for confidential data in the short term. Yet with some forethought it is possible to avoid a data breach even during times of crisis.

"At Shred-it we believe that prevention is the best planning tool," says Robert Guice, Shred-it's Executive Vice President, EMEA.

"To avoid an information breach, it is essential that all information, both electronic and paper, is secured wherever it is located and all information that is no longer needed destroyed in accordance to data privacy legislation."

In this Issue

Small businesses especially at risk

The private sector has a vital role to play in the protection of our personal information yet smaller organisations tend to focus far less on data security and do not have in place formal information security policies and procedures. According to information security and forensic computing consultancy 7Safe 66 per cent of data security breaches occur within organisations employing less than 100 people.

SMEs:

- Rarely have a dedicated HR function to hold and protect employee records.
- Often have no restrictions on the internal information that can be accessed by employees, including temporary staff.
- Typically do not carry out security checks on their potential employees during the hiring process.
- Do not have the resources to outsource their data security requirements.

However, many SMEs cannot afford the financial blow of a security breach, with the National Fraud Authority estimating that fraud costs the UK's private sector £9 billion annually.

Information security recommendations from Shred-it

There are just two important principles behind best practice in secure document management for SMEs to adopt which is as follows:

✓ All sensitive information should be stored securely until destroyed.
All sensitive information that is no longer required should be destroyed immediately

Shred-it advocates a tight chain of custody around the entire document management process, which should be implemented in a strategic, systemic way. Below is a list of best practice that forward-looking organisations follow to protect themselves, their clients, employees and other stakeholders both during normal operations and during an emergency.

01 **List all information security risks:** specific to your organisation, targeting both paper-based and electronic information sources; consider every stage of the information cycle, from data generation and storage to the transfer of data from location to location and the document destruction process.

02 **Develop data security strategies:** that address each of these risks.

03 **Commit to total information security:** have a clear vision of why your organisation is implementing these measures and have the systems in place to make it happen – clear policies, and appropriate communication, training, and management processes.

04 **Train your staff** in document destruction policies and best practices; offer training courses on general security or specifically deal with secure document destruction. Best practices can be summed up as four principles that are easy to understand:

- **Shred all documents** – to avoid the risks of human error or poor judgment.
- **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 once confidential paper waste is at the recycler.

http://www.media-awareness.ca/english/issues/privacy/canadian_legislation_privacy.cfm.

Shred-it's 2009 customer research.

Shred-it's 2009 customer research.

Sign up for your free data security audit

As security and public safety threats are more immanent than ever, the need for secure continuity planning is a requirement of today's workplace. Let us help you to assess your current process and provide best practice guidelines to help you mitigate the risk of a data breach.

To learn more about Shred-it services or to book your FREE security audit, visit http://www.shredit.co.uk/

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 services 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.

To learn more about Shred-it document destruction service, contact us at: **0800 028 1164**