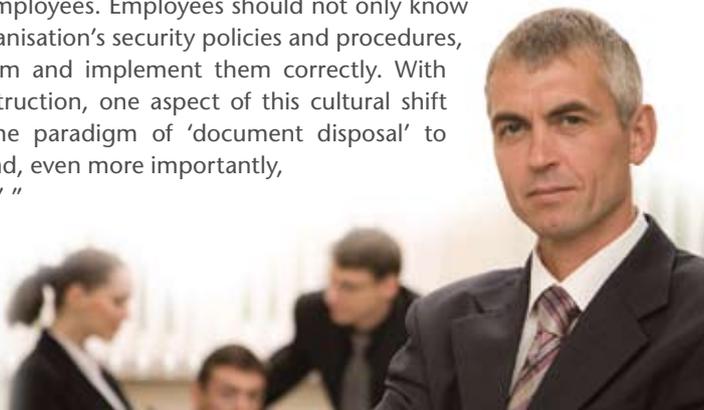


Document Destruction: How to create a total security culture in your organization

“There is a growing need for secure document management and destruction as a preventative measure against information security breaches,” says Michael Skidmore, Chief Security Officer at Shred-it. “Effective protection comes hand in hand with an organisational culture of total security, which requires a shift in the attitudes of employees. Employees should not only know and understand their organisation’s security policies and procedures, but truly commit to them and implement them correctly. With regard to document destruction, one aspect of this cultural shift is moving away from the paradigm of ‘document disposal’ to ‘document destruction’ and, even more importantly, ‘destruction at the source.’ ”



Welcome to the fourth edition of Securing the Future, a periodic newsletter from Shred-it. In this issue, we will talk about the importance of education and awareness when it comes to information security – and pinpoint some common concerns and best practice solutions that will help you create a high-security culture in your organisation.

IN THIS ISSUE

- “Insider Breaches”: why security concerns have shifted “inside”
- Changing the stakes: the effect of the recession on security programs
- High-security culture starts with employee education
- Effective security solutions eliminate the risks at the source
- How to create a total security culture: practical tips



“Insider Breaches”: why security concerns have shifted “inside”

It may come as a surprise to many that insider access to sensitive data, including customer and employee records, is a major security concern, potentially leading to identity theft and fraud. According to the “Executive Guidance for 2010” report from global executive network and consultancy Corporate Executive Board, organisations globally lose an estimated seven per cent of annual revenues to employee fraud.

These figures point to the conclusion that organisations need to turn inward when dealing with security threats. Consider who has access to sensitive information in your organisation. Given that employees with “access” are so closely related to potential risks for leaked or lost data, stringent access policies should be in place and be followed through rigorously. While there are no sure-fire methods for preventing security breaches from within, there are ways to reduce the threat– and creating a total security culture is one of the key components of any successful strategy.

High-security culture starts with employee education



While each and every organisation has unique security challenges, it is essential that employee education is at the forefront of any security policy in the workplace. In particular, educating employees on what documents need to be securely destroyed is key, since according to the aforementioned research by Fellowes in 2009, nearly one-third (32%) of employees admit to always throwing sensitive documents directly into the rubbish bin.

... and flows from top management

According to Fellowes' research, 71% of UK employees think their companies should do more to ensure confidential documents are handled responsibly. For a real movement towards total security, initiatives should start from the top with the adoption of high-security strategic thinking amongst the senior management team, who can then push it down the organisation in the form of effective security policies, processes and values. A lack of a strategic security planning, combined with weak or inconsistent implementation of an organisation's security policies and procedures, does nothing but create a working environment that is more susceptible to security breaches.

Changing the stakes: the effect of legislation on security programs

With fraud on the rise amidst the ongoing recession, data security is now more important than ever for UK businesses looking to protect their financial standing and corporate reputation. The potential costs of a data security breach could run into millions of pounds, leading to dented credit ratings, angry or lost customers and irreparable damage to client trust. However as the recovery from the economic recession is just starting, many organisations are still showing a reluctance to increase or even sustain their security budgets. According to independent research commissioned by Fellowes in 2009, only 64% of UK businesses have put in place a clear policy on how

to handle documents with sensitive information. The question arises: are scaled down security measures enough to deal with the growing threats of security breaches?

"The high-security culture does not necessarily mean an increase in budgets or more effort," says Robert Guice of Shred-it. "In many cases, it simply means changing your processes and thinking differently. The first step towards a culture of high security, so critical to the integrity of any organisation's confidential data, is to understand the big picture of the organisation's typical security risks and then assess the best way to address them."

Effective security solutions eliminate the risks at the source

Documents should be protected from the moment they are created until the time they are no longer needed. After all, prevention is always better than cure. Rather than focusing on security measures after a security breach has occurred, organisations should look to the future to develop approaches and concepts that are strategic, integrated and long-term, such as eliminating security risks at the source and ensuring security across each document's entire lifecycle.

One of the most effective ways to prevent security breaches from either inside or outside an organisation is by implementing "shred all" policies. A "shred all" policy will make sure that all documents are fully and securely destroyed on a regular basis.

The cultural shift should change from reducing, to eliminating security loopholes throughout the lifecycle of any given document. Rather than "disposing" or "discarding" of confidential data that is no longer needed, employees should be trained in the values of "destruction at the source".



How to create a total security culture: practical tips

A culture of security in the workplace is about educating employees about the importance of secure document management and destruction. The attitudes and values reflected in your organisation's security strategies, policies and procedures are the foundation of this security culture.

The tips from Shred-it below will help you build the culture of total security in your organization:

- Identify all potential risks that may threaten the security of your organisation's confidential information, including customer, business and employee-related documents.
- Examine the document workflow and lifecycle, from data generation and storage to data transfer and, finally, document destruction; analyse both electronic and paper-based sources.
- Create a comprehensive information security strategy for all areas of your business.
- Build an organisational culture that values and respects confidentiality and privacy.
- Develop security policies that are compliant with the Data Protection Act and all other relevant privacy legislation for your industry.
- Restrict access to confidential data, in electronic and paper form, based on specific business needs of specific categories of personnel.
- Train your staff in secure document management and destruction; implement "shred-all" policies and "destruction at the source" values, making sure all paper documents are securely destroyed on a regular basis.

In the UK alone, Shred-it has 15 branches, employs over 200 people and operates 107 shredding trucks, providing the most secure and trustworthy data destruction services possible for its clients. Shred-it UK has clients which span the sectors, from government agencies to financial and legal institutions, taking each customer's unique needs into account and bringing secure on-site document destruction services direct to their door, thus ensuring total confidentiality in security and shredding.

Shred-it is a world-leading document destruction company that ensure 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 500 police forces, 1,500 hospitals, 8,500 bank branches and 1,200 universities and colleges.



Making sure
it's secure.™

To learn more about Shred-it document destruction service, contact us at: **0800 028 1164**
or visit our website at **www.shredit.co.uk**.