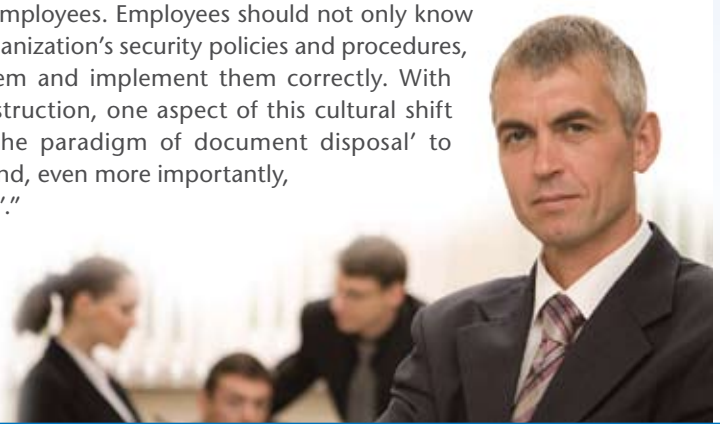
SECURING THE FUTURE

Shred-it®

VOLUME 1, ISSUE NO. 4 | WINTER 2010

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 organizational culture of total security, which requires a shift in the attitudes of employees. Employees should not only know and understand their organization'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 organization.*

IN THIS ISSUE

- "Insider Breaches": why security concerns have shifted "inside"
- Changing the stakes: the effect of legislation on security programs
- High-security culture starts with the correct assessment of risks
- 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 key organizational security concern, potentially leading to identity theft and fraud. The Ponemon Institute recently reported that 85 percent of U.S. organizations have experienced at least one data breach in the last 12 months. The report also revealed that the number of companies experiencing more than 5 data breaches in one year rose to 22 percent in 2009, up from 13 percent in 2008.

These figures may point to the conclusion that organizations need to turn inward when dealing with security threats. Consider who has access to sensitive information in your organization. Given that employees with "access" are most closely related to potential risks for leaked or lost data, stringent access policies should be in place and followed rigorously. While there are no guaranteed 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.

Changing the stakes:

the effect of legislation on security programs

The eminent threat from fraud artists who benefit by stealing vital business and personal information makes your organization's confidential data vulnerable to security breaches – potentially exposing your customers, clients or employees to identity theft and fraud.

Data security should be a top priority in your organization to maintain good business standards. According to the latest research from The Ponemon Institute, 58 percent of U.S. organizations reported that data protection is a very important part of their overall risk management strategy.

Organizations should also consider recent legislative actions that are requiring businesses to make information security a major business priority.

The U.S. Federal Trade Commission is in the process of implementing the Red Flags Rule, under the Fair and Accurate Credit Transactions Act (FACTA). The rule requires covered organizations to implement programs that identify and detect the warning signs of identity theft. Organizations that must comply with the rule include all state and national banks, savings and loan associations, mutual savings banks, credit unions and any other organization or person that holds a "transaction account." Enforcement of the Red Flags Rule was recently delayed for the fourth time to June 1, 2010. The question for all organizations covered by Red Flags Rule requirements is: will they be prepared to comply when the implementation deadline arrives?

Another regulatory rule was recently fulfilled on September 23, 2009 by the Federal Trade Commission. Until recently, the Health Insurance Portability and Accountability Act (HIPAA) did not require covered entities (including group health plans and healthcare providers) to notify individuals when their "unsecured" protected health information (PHI) had been breached. The new data breach rule, officially called HIPAA 2.0, mandates that organizations notify individuals when their information is exposed. In addition, if the breach involves 500 or more individuals, the organization must also notify the media and the Department of Health and Human Services immediately.

For organizations that must comply with these legislative requirements, proactive steps must be taken to protect and keep confidential the private information of customers and their own business. In this day and age, organizations must protect themselves and their customers from breaches that could cost millions of dollars in fines, capital and reputation.

High-security culture starts with the correct assessment of risks

While each and every organization has unique security challenges, many organizations' main concerns relate to the following:

- Disclosure or loss of confidential data
- Compliance with government regulations and legislation
- Business continuity and disaster recovery
- Loss of confidential strategic corporate information
- Employee understanding and compliance with security policy

… and flows from top management

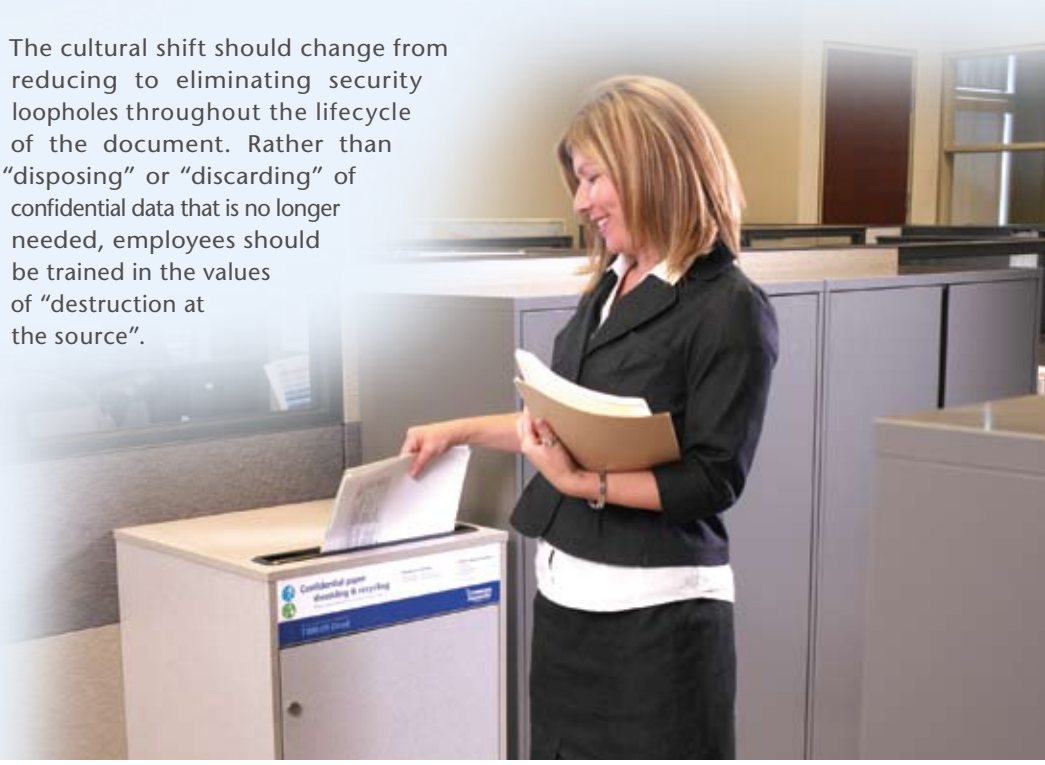
A lack of a strategic security planning, combined with weak or inconsistent implementation of an organization's security policies and procedures, creates an organizational environment that is more susceptible to security breaches. The culture shift towards total security, therefore, should start at the very top with the adoption of high-security strategic thinking amongst the senior management team, who can then push it down the organization in the form of effective security policies, processes and values.

Effective security solutions eliminate the risks at the source

Any solutions to the risks of security breaches should be based on a holistic, integrated perspective on document security throughout the document lifecycle across an organization. In other words, documents should be protected from the moment they are created until the time they are no longer needed. Organizations should look to the future as an opportunity to develop approaches and concepts that are strategic, integrated and long-term, such as eliminating security risks at the source and permanently securing the entire document lifecycle across all organizational units.

One of the most effective ways to prevent security breaches from either inside or outside an organization 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 the 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 is about educating employees about the importance of secure document management and destruction. The attitudes and values reflected in your organization's security strategies, policies, procedures and overall security thinking are the foundation of this security culture. Build an organizational culture that values and respects confidentiality and privacy.

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 organization'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; analyze both electronic and paper-based sources.
- Create a comprehensive information security strategy.
- Develop security policies that are compliant with national identity theft and privacy legislation.
- 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.
- Build an organizational culture that values and respects confidentiality and privacy.

SEC19704.1209.R1

Making sure it's secure.™

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 service 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:
1-800-69-Shred (74733).
www.shredit.com