SECURING THE FUTURE

In this Issue

- Have you reviewed your document destruction process?
- Implement document destruction policies and protocols
- Train your employees
- Request your free security consultation

Security breach?
It'll never happen to me.

U.S. small businesses need to take proactive measures to avoid risk.

In this issue we will take an in-depth look at new insight into the security habits and attitudes of small and medium sized businesses operating in the United States.

The results from an independent survey – the Shred-it *Information Security Tracker* conducted by Ipsos Reid and commissioned by Shred-it across Canada, the U.S. and the UK – indicate that while U.S. small businesses recognize the risk of security breaches within their organizations, most aren't regularly reviewing their security processes, conducting audits or training employees to help safeguard the business' confidential information.

According to the 2013 Shred-it *Information Security Tracker*, **40%** of small business owners have no protocols in place for securing data, a **5%** increase from last year.

Have you reviewed your document destruction process?

The risk of printed information falling into the wrong hands remains a constant threat, despite increased use of technology and computers to exchange information. Files may be shared electronically, but printed copies are still the norm and the information they contain is often easier to obtain than the originals saved on a computer.

In assessing how often small businesses reviewed their processes on secure document destruction, **30.2%** of U.S. respondents had done a secure document destruction review in the past six months, however, **25.1%** had never reviewed their processes.

Having a secure document destruction process in place and ensuring employees are trained and follow the process is critical to the security of sensitive information.

Implement document destruction policies and protocols

While **96.2%** of U.S. respondents said that keeping business information secure was important and having secure document destruction policies in place was important, **55.6%** of organizations said they do not offer secure document security facilities such as secure locked consoles.

In order to avoid the risk of a data security breach it is important that small organizations implement information security policies and protocols:

- Introduce a “shred-all” policy that means all unneeded documents are fully destroyed on a regular basis.
- Conduct a periodic information security audit.
- Don’t overlook hard drives in computers or photocopiers. Erasing your hard drive does not mean that the data is gone. Physical hard drive destruction is proven to be the only 100% secure way to destroy data from hard drives.
- Hire a reliable vendor that is well-informed and keeps you compliant with pertinent legislation, training requirements, etc. Finding a vendor that provides you with a certificate of destruction upon completion is ideal.

Back to the Top

Train your employees

Implementing policies and procedures is one thing, but it is also important that all employees are aware of the information destruction procedures and trained on a regular basis. According to the Shred-it *Information Security Tracker* results, **79%** of U.S. respondents admitted they were aware of the legal requirements of storing, keeping and disposing confidential data, yet more than 1/3 of the small businesses never train staff on the company's information security procedures and protocols. The results also showed that **48%** of companies have no one directly responsible for management of data security.

Ensuring that information security is taken seriously at every level within a business is vital to minimizing the risk of exposure that could lead to a data breach. Safeguarding data does not need to be an onerous task and there are simple steps any organization of any size can take to minimize the risk.

These include:

- Securely shredding confidential data – not simply placing it in recycling bins.
- Having a locked confidential paper receptacle in your office will ensure that no one has access to sensitive documents after they have been disposed.
- Limit physical access to storage closets and online access to sensitive or confidential files.

By taking such steps and regularly reviewing security policies, organizations large and small can protect themselves from the significant long-term impact of a data breach. If staff are not aware that there are policies and procedures in place, mistakes may occur, which could prove potentially fatal to the future of the business.

Back to the Top

SECURING THE FUTURE

Your FREE Security Consultation

Shred-it has developed an online survey to help businesses better understand security gaps, conduct your own security self-assessment.

Learn more about Shred-it services or book your FREE security assessment.

You can also visit Shred-it on LinkedIn, Facebook or follow us on Twitter.

Back to the Top

About Shred-it

Shred-it is a world-leading information security company providing document destruction services 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, more than 500 police forces, 1,500 hospitals, 8,500 bank branches and 1,200 universities and colleges.