SECURING THE FUTURE

Shred-it

Working outside the office is a growing trend

According to a recent study conducted by Ernst & Young, there will be approximately 46 million telecommuters worldwide by 2011. 2 As this phenomenon looks set to establish itself as a definite trend, organizations that fail to adequately plan for those employees who wish to work outside of the traditional office are putting themselves at risk of security breaches. Such breaches can be the result of technical or human error ranging from insecure internet services, lost or stolen USB devices or failure to shred paper-based documents. Despite the increase in employee numbers working outside of the office, staff may not be aware of how company or client data may be at risk of a security breach.

"Allowing employees to work from home locations, or while traveling outside of the office in general, is a greater threat to security than most companies realize," says Vincent R. De Palma, President and CEO at Shred-it. "Unfortunately, without the proper encryption, firewalls and document destruction policies in place, employees working outside of the office could be leaving confidential information open to a security breach."

Welcome to the eighth edition of Securing the Future. Our focus this issue is on working off-site from home or on the road, and the challenges associated with this. With an increasing number of employees looking to work more flexibly we will explore the information security issues associated with the non-traditional office, specifically examining what organizations can do to balance the needs of their staff to work flexibly with the needs of the organization to remain secure at all times.

Today's technological advances mean that staff can benefit from greater accessibility to company files, directories or confidential information, allowing them to work while traveling or telecommuting, and a significant number – 11.3 million U.S. employees – report that they work from home. 1 Connected laptops, USB devices, broadband internet and smart-phones all of course help facilitate this connectivity, ensuring that efficiency is maintained in a cost efficient, convenient manner. However, many businesses may not be aware that offering out-of-office access to confidential data brings with it a number of issues that need to be mitigated if data security is to be maintained.

In this Issue

Potential dangers of working off-site

While some businesses provide staff with secure, company-owned laptops, many workers, particularly those working remotely on an ad hoc basis, will be working from their own home computer. This poses a major concern for many businesses as home computers are unlikely to have the appropriate firewalls, data encryption or virus scanners typically installed on corporate-owned computers.

However, even a company-owned device installed with defensive technology designed to safeguard confidential data is not always 100 percent secure. Employees can abuse, or completely disregard how these tools should be used appropriately and effectively. According to a study by Ponemon Institute LLC, while business executives appear to overvalue encryption and its role to stop data breaches, many are actually hindering its effectiveness by improperly circumventing the technology, creating weak passwords, or using insecure wireless connections. 3 And to make matters worse, according to new research that identifies the most widespread concerns among the 100 largest U.S. technology companies, data security and data breach prevention ranks low as a risk factor. 4 Above all else, companies that don't insist on following strict policies for all employees that work outside of the office are creating an environment that relies on insecure information storage.

Which Businesses Are At Risk?

Regardless of size, any company which allows employees to take confidential information outside of the office is potentially at risk of a security breach. If your business allows employees to work from home or while traveling, or if staff are able to access social networking sites from a work device or store company information on USB keys, then your company information is at risk. While the focus may be on electronic documents, the risk associated with paper documents should not be overlooked. These can be misplaced, stolen or improperly destroyed, leaving company and client information exposed, which could increase the risk of a security breach. So what are the key areas of concern that lead to security breaches?

- Most large corporations allow employees to work away from the office, which means confidential documents, in both hard and electronic format are taken away from the security of the office.
- Employees working from home will be creating documents containing sensitive information (budgets, spreadsheets, client data, etc). Even if they delete these documents once complete, the document is not permanently removed from the computer hard drive memory.
- While electronic copies can fall into the wrong hands, the biggest risk of a security breach is still posed by hard copy paper documents. By their very nature, home-based businesses and small start-ups do not have the capacity that large businesses have to ensure security of their internet, electronic documents and hardcopies.

[3] http://www.itworldcanada.com/news/business-leaders-overvalue-data-encryption-study/140184
[4] http://www.priv.gc.ca/information/ar/200910/200910_pa_e.pdf

Get smart about working away from the office

Offering your staff the option of working remotely is seen as a real benefit by many employees looking to better manage their work/life balance. But ensuring that any employee working off-site is able to apply the same rigorous information security procedures as those working on site is a challenge. While technology and encryption is part of the answer, data loss and identity theft is too often caused by human error, not through a technical device. By creating policies that follow the document destruction life-cycle, ensuring that confidential data is safely and securely stored from the moment it is created, to the time it is no longer needed and destroyed, every organization can better protect its own business information and that of its clients.

Recommendations from Shred-it:

There are a number of ways an organization can secure its confidential data when employees are working off-site:

01 Prepare guidelines – either in-house or via a third party - on secure information destruction for employees working offsite.

02 Implement a shred-all policy for employees to ensure that all documents or other private information is securely destroyed to prevent the risk of a security breach.

03 Enlist the services of a third-party shredding company to visit employees that work off-site and pick up paper documents that are no longer needed. A third party shredding service will guarantee that documents are locked in secure consoles until shredded and then properly recycled.

04 Ensure that all files, laptops and internet connections are password-protected with a secure password and activated security settings and firewalls.

05 If employees must use a USB key, ensure that employees download EncryptStick encryption technology onto their USB. Combined with a user password, EncryptStick will ensure that your USB data is safeguarded in case the device is lost or stolen.

06 Ensure employees overwrite their data to make sure that it is completely deleted from their computer. Provide and run a hard-drive wiping software which will ensure that hard drives are totally clean.

Sign up for your free security consultation

As security and public safety threats are more intense than ever, the need for secure business continuity planning is clearer than ever.

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

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:**1 800 69-Shred (74733).**