SECURING THE FUTURE

In this Issue

Canadian Businesses are Deprioritizing Information Security

In this issue, we will discuss how Canadian organizations continue to be complacent about information security.

It's no secret that the improper disclosure of confidential information is risky and can cause damage to corporate reputations. In today's business climate, savvy business leaders know it simply makes good business sense to arm employees with tools and resources to safely manage information.

Shred-it's 4th Annual Information Security Tracker shows business leaders are taking little to no action to make information security a priority. In fact, the study shows that in some instances, information security policies have actually decreased. Considering the fact that Canadians are more aware of their information security risks than ever before, it's clear more needs to be done to motivate business leaders to take action.

According to the annual study conducted by Ipsos Reid:

- Only 46 percent of small business owners have an information security protocol that is strictly adhered to by all employees, and 31 percent admit to having no protocol in place at all.
- It's not only small business owners. Only 42 percent of c-suite executives admitted to having a protocol in place that is strictly adhered to by all employees and 22 percent admit to never training their staff on information security, a number which has risen significantly since last year.

SECURING THE FUTURE

When you consider that the average cost of a data breach is nearly $6 million, there is plenty of cause for concern. Organizations need to take more responsibility in safeguarding confidential information not only for their stakeholders, but also for their corporate livelihoods.

Are you doing enough?
To take control and properly manage your confidential data, keep the following suggestions in mind:

- Demonstrate a top-down commitment from management to the total security of your business and customer information.
- Implement formal information security policies; train your employees to know the policies and strictly follow them.
- Eliminate potential risk by introducing a "shred-all" policy; remove the decision-making process regarding what is and isn't confidential.
- Conduct a periodic information security audit.
- Introduce special locked containers instead of traditional recycling bins for disposing of confidential documents.
- Don't overlook hard drives on computers or photocopiers. Erasing hard drives does not mean data is destroyed. Physical hard drive destruction is proven to be the only 100 percent secure way to destroy data from hard drives.

Recent reports confirm that last year close to a million Canadians had their private information compromised by a data breach. It's clear that today, more than ever before, organizations need to prioritize information security by implementing protocols that help protect documents and hardware.

Mind the gap

The gap between policy and practice leads to weakness in information security.

Imagine what would happen to your organization if you lost personal information, including social insurance numbers, names and dates of birth, home addresses and telephone numbers for more than 500,000 Canadians?

SECURING THE FUTURE

For Employment and Social Development Canada (ESDC) it was a reality when a portable hard drive containing personal information for student loan recipients disappeared.[1]

An investigation by the Privacy Commission of Canada found the hard drive had been left unsecured with no data encryption or even a protected password; while the ESDC says there is no evidence the personal information stored on the hard drive was used for fraudulent purposes, for those 583,000 individuals whose personal information went missing, confidence in the ESDC has been tarnished with many questioning security protocols of other government departments.

Unfortunately, the ESDC is not the only organization lacking in cyber-security policies. Shred-it's 4th Annual Security Tracker revealed that most Canadian organizations don't have a protocol for destroying data stored on hard drives. According to the study, almost half of the small business owners surveyed had never disposed of hardware containing confidential information, and of the c-suite executives surveyed, half didn't know the proper method for destroying confidential data stored on hard drives.[2]

It is likely that the Privacy Commissioner of Canada's investigation will prompt other federal government departments to review their policies and practices, which is great news for everyone.

Three simple workplace guidelines are designed to safeguard hard drives:

- Perform a regular cleaning of storage facilities and avoid stockpiling unused hard drives.
- Destroy all unused hard drives using a third-party provider who has a secure chain of custody to help give you peace of mind and ensure your data is being kept out of the hands of fraudsters.
- Regularly review your organization's information security policy to incorporate new and emerging forms of electronic media.

What types of electronic media can be destroyed?

- Hard Drive (any kind of laptop, desktop, PATA, SATA and many more).
- Backup Magnetic Tapes (any kind of DLT, mini cartridges and many more).
- Floppy Disk (3.5 inch disk, 5.25 inch disks, and many more).

1 Office of the Privacy Commissioner 2014, Investigation into hard drive loss highlights important lessions for all organizations to follow
2 Ipsos Reid, 2014 Information Security Tracker

SECURING THE FUTURE

- Zip Disk (100 MB, 250 MB, and other large disks).
- Optical Media (CDs, DVDs, Blue Ray, and HD DVD).

For more information on tips for Federal Institutions Using Portable Storage Devices please visit the Office of the Privacy Commissioner of Canada's website — priv.gc.ca.

What should your company do in the wake of a data breach?

If your organization experiences a data breach, there are a few important steps that should be taken immediately:

- Seek expert legal assistance and advice.
- Take inventory of the data that has been impacted.
- Develop a targeted plan of action that includes clearly-defined steps.
- Carefully manage the flow of information related to the breach.
- Be prepared to communicate effectively to all stakeholders, including customers, partners, vendors, employees, the media and if needed, the Office of the Privacy Commissioner.

Quick corrective measures are essential, but it is also critical for companies to take proactive steps to prevent further breaches from occurring.

Contact Shred-it for a FREE security consultation

For more information on successfully implementing an information security program in your organization, visit the Shred-it Resource Centre at shredit.com/resource-centre

You can also stay informed with Shred-it on Facebook and LinkedIn or follow us on Twitter at @Shredit.