SECURING THE FUTURE

In this Issue

- What laws protect you?
- How is your information stolen?
- How can you protect your business identity?
- Request your free security consultation

Business Identity Theft: A Real Threat to Canadian Companies

For organizations of all sizes, preventing fraud is better than dealing with the tough consequences. In this issue we will discuss the growing threat of identity crimes directed against businesses and the legal response from the Canadian government.

As identity theft continues to be the fastest growing form of consumer fraud, government bodies have made the protection of personal information a priority. However, a growing trend is proving that it's not just customer data that thieves are after. Fraudsters are now obtaining information about companies and assuming their business identities in order to steal company assets, client lists and credit information or secure new business relationships and payments. Canadian companies, large and small, are vulnerable to breaches in data security and risk financial damages and reputational losses resulting from business identity theft.

Research by the Canadian Anti-Fraud Centre shows that there were over 4,500 identity theft victims and more than 17,000 reported cases of identity fraud in Canada in 2011, with a total dollar loss of over $13,000,000[1]. Shockingly, it's estimated that these figures only represent 5 per cent of victims. In reality, identity theft is a serious criminal activity that is not only becoming increasingly lucrative, but

1 http://www.phonebusters.com/english/documents/2011%20Monthly%20Stats%2012.pdf

SECURING THE FUTURE

is easily happening across borders[2]. Identity thieves can be third-parties, employees, competitors and even suppliers – and they are using increasingly sophisticated measures to steal confidential business data and commit business identity fraud.

With all the risks associated with data breaches, why don't more business owners report the theft of company information? In some cases, large companies don't notice small breaches in their data security structures until after fraud has been committed. Medium-sized and small business owners often don't report information breaches, because they believe that their operations would be adversely affected if the breach were publicized. Finally, according to a Globe and Mail report, there is little incentive for companies to report business identity theft committed against them because law enforcement tends to prioritize the investigation of consumer or individual identity theft over that of businesses.

What laws protect you?

In 2009, Bill S-4 created three new core Criminal Code offences targeting identity-related crime, including obtaining and possessing identity information with the intention of using it unlawfully, trafficking in identity information and unlawfully possessing or trafficking in government-issued identity documents.

These amendments to Canadian identity crime law also created a new sentencing power, where courts can order offenders to pay restitution to identity theft or identity fraud victims. The restitution is based on the costs needed for the victim to restore their identity, such as the cost of replacing identity cards and documents as well as correcting their credit history. The courts also have an existing ability to order restitution for actual economic or property losses[3]. However, it is also important to note that Bill C-29, a 2010 amendment to the Personal Information Protection and Electronic Documents Act (PIPEDA) clarified that existing provisions against the sharing of individuals' personal information do not apply to business details.

2 http://www.justice.gc.ca/eng/news-nouv/nr-cp/2010/doc_32471.html
3 http://www.justice.gc.ca/eng/news-nouv/nr-cp/2010/doc_32471.html

SECURING THE FUTURE

How is your information stolen?

Theft of paper documents and electronic data occurs in many forms, from dumpster-diving to hacking into company networks. Often, fraud is committed when files are left out in the open and visitors are able to steal, copy or snap a photo of information that should be kept confidential. Furthermore, some organizations do not take proper steps to securely destroy their private data.

The growing mobile workforce and shift to cloud computing are leaving organizations increasingly vulnerable to electronic security breaches and the theft of sensitive business data online. A 2011 RCMP report warned that security risks were rising as more and more businesses are choosing to cut costs by switching to cloud computing for the storage of their information. This leaves business information stored in remote third-party servers, which are sometimes in an online space that can be hacked or accessed by fraudsters, and that are also regulated by the laws of other countries that cannot be enforced in Canada[4].

How can you protect your business identity?

Consider how identity thieves are stealing the information required to assume a company's identity and take steps to prevent it. Here are some tips to help you ward off fraudsters:

- Prevention is the best protection. Instead of just dealing with identity theft as it occurs, develop preventative approaches that are strategic, integrated and long-term, such as eliminating security risks at the source and carefully monitoring and restricting access to information.
- Develop internal policies and protocols that mandate secure document storage and disposal practices.
- Shred everything on a regular basis. By implementing "shred all" policies, you avoid the risks of human error or poor judgment about what needs to be shredded.
- Create a culture of security by educating employees on information security best practices.
- Shred using a professional service. It's the only way to ensure there are no security loopholes anywhere in the process.
- Ensure your electronic data is protected by securely and safely destroying your hard drives and photocopier.

4 http://www.montrealgazette.com/technology/Cloud+shrouds+fraud+risk+RCMP/6142832/story.html

SECURING THE FUTURE

Your FREE Security Consultation

To conduct your own security self-assessment, Shred-it has developed an online survey to help businesses better understand security gaps on their website at the following link:
http://www.shredit.com/Shredding-Service/Risk-Assessment-Survey.aspx

To learn more about Shred-it services or to book your FREE security assessment, visit www.shredit.com

You can also visit Shred-it on Facebook or follow us on Twitter at @Shredit.

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.