

VAQ

Read more articles from the VAQ –
Value Added Quarterly Business Journal



How safe is your business?

Identity theft is growing in Canada, and businesses should take precautions.

Michael Geist, Canada Research Chair in Internet and e-Commerce Law, University of Ottawa Law School

A recent report by Criminal Intelligence Service Canada says emerging technology is enabling identity theft, making it one of North America's fastest-growing crimes. Canadian and U.S. law enforcement agencies have reported an increase in identity theft as a means of furthering or facilitating other types of crime, from organized crime to terrorism, and businesses as well as individuals are increasingly vulnerable.

Phonebusters, Canada's fraud reporting agency, reports losses from identity theft totaled \$21 million in 2003 — almost double the figure from the previous year. The Better Business Bureau of Canada estimates an annual cost of \$2.5 billion to Canadian consumers and the total annual cost to the Canadian economy has been estimated at \$5 billion.

Information can be stolen in many ways

Identity thieves use a variety of high and low tech means to steal information from businesses. Some criminals have broken into offices to take computer hard drives, bribed or compromised employees into obtaining personal data, or hacked into databases. "Dumpster divers" even rummage through trash to pick out bank statements and credit card receipts.

Criminals who want to obtain personal data online sometimes use a technique known as "phishing", the creation of e-mails and websites that appear to belong to legitimate businesses. Consumers who receive e-mails claiming to be from a legitimate business are often directed to a website where they are requested to enter large amounts of personal data. The criminals who created these e-mails and websites are not connected with the legitimate businesses and their purpose is to obtain the consumers' personal data for fraud schemes.

How Canadian business is responding

Professor Michael Geist, Canada Research Chair in Internet and e-Commerce Law at the University of Ottawa Law School, comments that today's businesses are increasingly challenged to guarantee the security of personal information collected and retained on employees and customers, as well as securing business transactions conducted online.

"The fact is, any information that's retained electronically is vulnerable to misuse, and businesses are caught in a balancing act between what is practical and taking adequate protective measures to mitigate the risk," comments Geist. "However, there is still a lack of awareness within the business community that maintaining an appropriate level of information security within the workplace should be a priority."



44 King Street West
Toronto, Ontario M5H 1H1
e-mail: businessproducts@scotiabank.com
www.scotiabank.com/vaq

How safe is your business?

Geist adds that while research on identity theft issues is still in the early stages, the topic is very much a going concern. The Canadian Bankers Association (CBA) recently advocated for new identity theft legislation. Among other changes, the CBA wants to see identity theft clearly defined in the Criminal Code. They also want to make it an offence to possess multiple pieces of other people's identification.

Protecting personal information

Canadian businesses should be aware that the Personal Information Protection and Electronic Documents Act (PIPEDA) came into full effect on January 1, 2004.

PIPEDA applies to all personal information collected, used or disclosed by private sector organizations in the course of commercial activity, and under its provisions, organizations must protect personal information with security safeguards appropriate to the sensitivity of the information.

Good information protection will not only help to reduce the likelihood and risk of unauthorized access to customer and employee data, but also enable businesses to comply with the new legislation. Organizations are encouraged to consult the various information sources available to guide them in adopting the necessary procedures to comply.

An excellent place to start is Industry Canada's "Privacy for Business" website (<http://privacyforbusiness.ic.gc.ca/epic/internet/inpfb-cee.nsf/en/Home>) to assess your organization's information handling practices, and highlight changes to information practices and systems you should implement where necessary.

Preventing identity theft

While no one would argue the need for preventive measures, Geist points out legal issues concerning identity theft are not simple.

"There are many organizations involved in researching the most pressing challenges associated with identity theft prevention, which is not simply a question of introducing new laws and implementing tighter policies to deter such fraud. These systems can result in invasion of privacy or violation of civil liberties, so there is considerable tension in trying to balance identity theft deterrence against loss of personal privacy," concludes Geist.

What businesses can do to reduce the risk of identity theft

So, what should a business do to protect itself?

The report provided by Criminal Intelligence Service Canada recommends the following tips and guidelines:

- Keep valuable customer data, such as credit card or bank account numbers, in a secure location.
- Shred or destroy paperwork no longer needed, such as bank machine receipts, receipts from electronic and credit card purchases, utility bills, and any other document from customer transactions that contains personal and/or financial information.
- If part of your business involves online transactions, check regularly to see whether someone has set up a "phishing site" in the name of your business. If you find a site, look up its domain name through registrar sites to find out which web-hosting service or Internet service provider the fake site is using, and contact that service or provider immediately.
- If your business has a website customers can use to order merchandise or enter valuable personal data, have your information technology group check regularly to ensure there are no security "holes" through which others can improperly access customer data.
- Regardless of what size your business is, decide on a fraud prevention and detection program you can afford and implement it promptly. Online businesses, which often depend on credit cards for payment, should consult the financial institutions with which they have merchant relationships and other payment-card associations as appropriate, to learn what programs or mechanisms may be most suitable for their businesses.
- Merchants who conduct business face-to-face with their customers should consider establishing a uniform policy of requiring more than one form of identification when a customer is paying by check or credit card.

Making sure you're maintaining an appropriate level of information security within the workplace should be a priority. In the end, the more you know, the more you can protect your company and ultimately your customers.



44 King Street West
Toronto, Ontario M5H 1H1
e-mail: businessproducts@scotiabank.com
www.scotiabank.com/vaq