

BUSINESS BC

EDITOR PAUL BUCCI 604-605-2520 • MONDAY, MAY 3, 2004 • E-mail sunbusiness@png.canwest.com

Business of protection

TECHNOLOGY | Stealing computer data can be worse than stealing a computer

Imagine that thieves broke into your business and stole a computer. The hardware, the software and, in time, the stored information could be replaced, and life would go on.

But what if that computer contained personal information about customers, employees or other individuals? If those records were not adequately protected, your company could be in for a long, costly lawsuit. Life might not go on after all.

Now consider that thieves need not physically break into your business to do it. Using everything from crooked employees to the Internet, organized criminals are increasingly targeting databases for the purposes of identity theft, a kind of fraud where thieves impersonate other people, usually to take out credit in their names.

That's the somewhat scary message Vaclav Vincalek and Larry Munn are taking to their clients and anybody else who will listen.

Vincalek is the president of Pacific Coast Information Systems, a Vancouver software and consulting firm. Munn is a partner with law firm Clark, Wilson. From their different perspectives in technology and law, they both see a huge potential liability for any company that keeps information on individuals.

CREDIT: Steve Bosch, Vancouver Sun



Larry Munn (seated) and Vaclav Vincalek see a potential liability for any company that keeps information on individuals.

But they also believe there are steps companies can take to minimize the risk not only of identity

theft, but also its legal ramifications.

The problem arises because electronic data storage is still in its

BUSINESS BC

EDITOR PAUL BUCCI 604-605-2520 • MONDAY, MAY 3, 2004 • E-mail sunbusiness@png.canwest.com

infancy, Vincalek said.

"Everything is so recent," he said. "Now we have technology which is so powerful yet we are so inadequately prepared to see it deployed among all the users."

The federal and B.C. privacy acts that took effect Jan. 1 notwithstanding, the law always lags behind the technology.

"As long as the world operated in a paper environment we weren't that concerned about identity theft because it was much, much harder to do," Munn said. By contrast, electronic documents are easily moved, copied or altered without anyone knowing until it's too late.

"Security for most companies means you lock your door at night and you lock your filing cabinets. I think a lot of companies forget that their biggest vulnerability now is if they do have a computer system or they're connected to the Internet," Munn said.

The threat came into abrupt focus in March when credit bureau Equifax Canada—what ought to be the Fort Knox of databases—revealed identity thieves had accessed the credit histories of 1,400 Canadians, mostly British Columbians and Albertans.

A case a year earlier where thieves in Regina stole a hard drive containing information on hundreds of thousands of Investors Group and Co-operators Life Insurance clients resulted in a class-action lawsuit claiming \$5 million in damages.

The same month as the Equifax breach, thieves obtained information on more than four million Japanese Internet subscribers with Softbank Corp. The company has since allocated \$37 million to compensate its customers.

In none of these cases has there been any report of abuse of the information stolen. But Vincalek and Munn believe it is just a matter of time before there are in these or other cases—and then the stakes will rise higher still.

Vincalek fears it will take a damaging information breach, followed by an even more punishing class-action lawsuit, before many companies hear the wake-up call.

"There will be something big and everybody will start paying attention," he said.

He personally recognized this growing problem of corporate privacy liability long before it hit the headlines, and six months ago contacted Munn to discuss ways to get the message out, and maybe develop a joint consulting practice in electronic security. Since then federal and B.C. privacy laws affecting virtually every company and non-profit organization have come into effect. PCIS plans to hold a seminar for its clients on the subject in June.

So how can companies protect themselves?

To start with, they should familiarize themselves with their obligations under B.C.'s Personal Information

Protection Act and the federal Personal Information Protection and Electronic Documents Act. Possible violations of privacy law would likely be the victims' first line of attack in a civil lawsuit, Munn said.

On the technology front, Vincalek advocates a "less is more" approach. Don't buy technology you don't need. Don't collect information you don't need. And don't feel you have to have the latest software; you're better off with tried-and-true second-generation versions.

Companies should also look at their operational procedures. Never give a password to somebody over the phone. Limit the number of people who have access to a database and the portion of the database they have access to. And treat personal information—even a simple name and address—as if it's your most closely held trade secret.

It might well add to the time involved and the cost of doing business, but that is a small price to pay for using technology that enhances productivity in other ways. □

mmcullough@png.canwest.com