Novell preparing to sell 10 per cent of its Corel stake

CANADIAN PRESS

TORONTO — Corel Corp.'s biggest shareholder, Novell Inc., says it will sell up to 10 per cent of its stake in the Ottawa software maker.

Novell, based in Provo, Utah, filed documents late last week with the U.S. SEC that say it plans to sell up to one million Corel shares over 90 days.

The company holds 9.95 million shares — or 16.3 per cent of shares outstanding — acquired in the spring of 1996, when Corel bought its WordPerfect software line. If Novell were to sell the entire one million shares, it would reduce its holding to about 14.7 per cent.

Novell official Jonathan Cohn said October trades won't be made public until Nov. 10, when Novell reports its trading activity for the month.

But John Hladkowicz, Corel's director of investor relations, said Novell officials told him they want to sell the shares by Friday, when the company's fiscal year comes to a close.

Trading in Corel shares was higher Tuesday than its three-month average on both the TSE and Nasdaq. In Toronto, 635,000 shares changed hands, compared with an average of 269,000 shares. On the Nasdaq, 415,000 shares were traded, compared with an average of 285,000.

Corel shares rose 40 cents to $4.90 in Toronto.

Corel stock has fallen sharply since early 1996, as it struggles to find a way to make a profit from the WordPerfect line. The latest blows came this fall, as the company unexpectedly revealed it would lose money in its third and fourth quarters.

DON'T OVERLOOK SECURITY

Satnam Purewal

Today's businesses rely on laptop computers for much of their information storage and transmission. That information is more valuable than the computer it's in.

Industrial espionage has been made much more convenient with the increasing use of laptop computers and by businesses restructuring for the global market.

People are mobile and, with high-speed communication lines, so is information. Today's business travellers must be more cautious with confidential information, and they must keep careful watch on their laptops.

Laptops are hot items with thieves these days. While replacing a high-end laptop is not cheap, the price is small compared with trying to replace the information on that laptop. If the information falls into the hands of competitors, the business impact could be even more costly.

Most people still do not back up their information on a regular basis and frequent flyers are even less likely to follow regular backup procedures. Business travellers must remember to back up their information regularly and then to store the backup disks apart from the computer. Storing backups in the computer bag is unacceptable.

According to *InfoWorld Canada*, about 265,000 laptops were stolen last year, a 50-per-cent increase from 1994. Airports pose the biggest risk.

Laptops are frequently stolen when fliers go through security, because this is when computer and owner are separated.

Experts recommend asking for a hand inspection. It takes a few minutes longer, but not nearly as long as it would take to recover your information.

Business travellers usually make use of the time before boarding to make calls. They put their computer down and concentrate on business. This makes them vulnerable, and the thieves know it. Within seconds, the laptop can be gone and its owner will only notice its disappearance when the call ends.

Hotel rooms are also areas of risk. Several years ago, two information security professionals presented a seminar on industrial espionage at a conference. The night prior to their presentation, they went through the hotel's garbage and were able to obtain confidential documents disposed of as regular garbage by conference attendees.

Most offices have policies regarding the disposal of confidential material. When individuals are out of town, they have no container designated for confidential shredding. Travellers must be aware of the type of material they are tossing out. If it would treated in a special manner at home, then it probably should not be put in with the hotel garbage without some sort of shredding.

Even on an aircraft, the business traveller is not safe from espionage. Some European airlines have reported bugging devices planted in business-class headrests in an attempt to obtain industry secrets when colleagues converse during flights. International corporations have responded by establishing procedures that seat colleagues separately.

Business travellers must also be alert to the risks posed by communications with distant colleagues. On the road, faxes and e-mail are favoured forms of communication. When faxing confidential information from external sites, stand by and watch it being sent. Many fax machines print confirmation or error messages with a partial copy of the fax to assist if there is a problem. Anyone who reads the confirmation or error message will be aware of the first page of the fax.

In my opinion, organizations increasing their international presence need to ensure their employees are aware of the risks they face when they are on the road. Such organizations should begin by developing polices to address these risks. They should then incorporate them into their security-awareness program.

Satnam Purewal is a senior consultant in the management solutions practice of Deloitte & Touche, specializing in Computer Security. She can be reached at (604) 640-3080 or through e-mail at spurewal@deloitte.ca