

Do Employees Have Their Hands in Your Pocket?

Vicki O'Brien, August 1, 2007

Access denied

It's quite likely that Vaclav Vincalek can walk into your reception area, open his laptop, access your file server and download your most sensitive corporate data in a matter of minutes. "If I wanted to, I could send it who knows where to who knows who and there would be zero way to trace it."

Vincalek, president of Pacific Coast Information Systems Ltd., a Vancouver software consulting firm specializing in electronic security, routinely demonstrates his skill for astonished clients, who didn't know their crucial, confidential data was quite so vulnerable to hackers and disgruntled employees out to sabotage systems or steal valuable corporate records. He then recommends ways to plug the leaks with advanced security tools such as firewalls and intrusion-detection systems.

Companies are required by law to safeguard private employee and consumer information. However, organized crime is increasingly targeting databases, often accessing them through crooked employees, as fodder for identity-theft scams.

It's ironic that the same technological advances that have revolutionized the world of work have also made things easier for white-collar thieves.

And it isn't just criminal outsiders who screw you over. A recent study of 900 IT professionals in different sectors conducted by online survey provider zoomerang.com found that almost half take data with them when they change jobs – including documents, lists, sales proposals and contracts. Some simply email information to a personal address; others walk out carrying the data, usually on peripheral storage devices such as portable memory sticks, flash drives or iPods, tucked away in a bag or pocket.

Tightening systems

Security should never hinder efficiency, says Vincalek. Rather than installing passwords on everything and driving your people crazy, he recommends investing in new security, such as devices with fingerprint scanners authenticated only to certain systems or portable

ID cards that lock users out of the system when they walk away from their work stations. Employers should also keep tabs on their own systems teams, he says. If the individual responsible for IT security leaves your organization on a bad note, he or she can effectively shut your business down.

Vincalek urges employers to think of an external form of insurance. "If you have files that would sell on the black market for \$1 million, how much are you willing to spend to secure them? Losing data is essentially the same as having your money stolen."

BC Business Online

Article interview with Vaclav Vincalek, Founder & President of Pacific Coast Information Systems Ltd. (PCIS)
<http://www.bcbusinessonline.ca/bcb/top-stories/2007/08/01/hands-your-pockets>



Pacific Coast Information Systems Ltd. (PCIS)

Suite 700 - 1112 West Pender Street
Vancouver, BC V6E 2S1 Canada
Tel: 1.604.844.7558 | Fax: 604.844.7508
Email: info@pcis.com
Monday to Friday (9am to 5pm PST)