

TECHNOLOGY: CYBERCRIME

Insurers look to cover hacking damage

Sophisticated privacy breaches and theft create new market in covering expensive data loss

JANET MCFARLAND

March 13, 2008

Insurers are betting that an explosion of sophisticated computer hacking will create a new market in Canada for insurance to cover the growing costs of recovering from privacy breaches.

Toronto-based **Executive Risk Insurance Services** says it is launching a new category of insurance for corporate clients, similar to products offered by U.S. giants like American International Group Inc. and Chubb Corp., to manage the fallout when sensitive data is lost or stolen.

The policies pledge to cover not only the straightforward costs of repairing computer damage, but also the far greater costs of notifying and reimbursing customers or compensating credit card companies for losses that occur from the fraudulent use of data.

David Griffiths, senior vice-president at insurance broker AON Reed Stenhouse Inc. in Toronto, says only a few Canadian companies have signed up to buy specialized privacy breach insurance, while most are still focused only on their computer security systems.

But with a flurry of high-profile frauds hitting some large companies over the past year, he believes the time has come for insurance to explode in popularity.

"It's an emerging risk that more and more boards are becoming aware of," he says. "Some products have been around, but a lot of clients are only starting to really take notice and say, 'All right, maybe we will take that next logical step and insure against the risk.' "

Brian O'Higgins, chief technology officer at Ottawa-based Third Brigade Inc., a security software company, says it is impossible for a company to have a foolproof computer system that cannot be breached, and companies like his cannot make security products fast enough to eliminate all the risk. He advocates insurance to cover the gaps.

"We've come a long way from the teenage hacker who's doing it for street cred to brag to his friends," he said. "It's now a criminal activity and making money is the motive behind all this."

In some cases, criminals are stealthily infiltrating systems to collect data for long periods of time, compounding the damage and the costs for companies that are victimized.

TJX Cos., parent of retailers such as Winners and HomeSense, disclosed last year that hackers had taken information from at least 45.7 million credit and debit cards after

breaking into its system in July, 2005, and collecting data back to 2003. The hackers continued undetected until the end of 2006.

TJX took a \$119-million (U.S.) charge last year to cover costs from the intrusion.

Many Canadian companies and agencies have also reported various sorts of privacy breaches over the past year, including Canadian Imperial Bank of Commerce, Club Monaco, Passport Canada, Bell Canada and Rogers Communications Inc.

Toronto-based Executive Risk, which specializes in directors' and officers' liability insurance, says its new privacy breach insurance, which is backed by Lloyds of London, will pay companies' costs to notify customers and cover customers' costs of repairing credit damage. Companies would also be covered for third-party costs, such as compensating credit card companies for their losses - a major expense in the TJX case.

The policies will also cover companies for their crisis management, including creating websites or call centres for affected customers or hiring public relations professionals to manage communications.

Jon Ashall, senior vice-president of corporate development at Executive Risk, says potential customers for insurance include retailers, financial institutions, utilities, health care providers or charities because all maintain databases of information that are especially valuable for criminals.

He said Executive Risk has tailored its coverage to Canada's privacy laws, which include strict new standards for companies to safeguard confidential information. The insurance package will also cover costs of dealing with regulators or paying fines.

And while Canadian privacy laws do not require mandatory notification of customers whose data has been stolen, Mr. Ashall says it has become accepted as a "better practice" and the expense will be covered by insurance. "I think there are a number of gaps in traditional insurance and the policy we're designing is intended to fill those gaps."

The insurance field is still new enough, however, that it is unclear exactly how much coverage companies need to cover all possible costs from a major privacy breach, says Ben Maidment, cyber and technology underwriter at Brit Insurance in London.

He said he has seen large companies buy policies to cover as much as \$150-million of costs, but said most small or medium-sized companies are buying \$10-million to \$20-million of coverage.