itbusiness.ca
Business Advantage through Technology

Print

Canadian IT security survey uncovers paradoxes, ironies

IT threats continue to grow but Canadian firms keep slashing security budgets. Insider breaches are on the upsurge yet local organizations are concentrating their efforts on fighting malware instead. A Telus-Rotman IT security survey explains why.

10/9/2009 6:00:00 AM
by Nestor E. Arellano

Reports of IT threats continue to grow but Canadian firms keep slashing security budgets, according to a study.

Insider breaches are on the upsurge yet local organizations are concentrating their efforts on fighting malware instead. In these uncertain times you would think that companies would think twice about outsourcing, but reports indicate a majority of Canadian businesses are preparing to do just that.

A recent survey of IT security practices across the nation carried out by Telus Inc. and the Rotman School of Management of the University of Toronto brought up these and other paradoxes.

"The bigger your business gets the worse threats you're bound to encounter. Ironically your security budget is not going up," sums up Ben Sapiro, research director, security practices, for Telus Security Labs, in Toronto.

Related stories:

How to effectively slash your IT security budget

Outsourcing the answer for GMAC Residential Funding of Canada

Cloud control – Top cloud computing risks and how to handle them

Sapiro presented key findings of the survey during his presentation titled: "Smashing the Stats for Fund and Profit" at SecTor a Toronto-based comptuer security conference on Wednesday.

Security budgets gutted

The number of data breaches quadrupled from 3.2 last year to 11.3 per organization in 2009. Annual losses due to data theft have increased from $293,750 in 2007 to $807,310 on average this year, the Telus researcher said.

Yet IT security budgets are heading south.

More than 75 per cent of companies polled said they decreased their security budget by as much as 10 per cent. Only 25 per cent of the respondents reported budget increases in 2009.

This seeming paradox, Sapiro said, could be explained by technology advances and economic developments. Recent deployment of improved risk detection technologies have provided many companies with enhanced insight into threats affecting their organization.

"Companies are able to report more breaches because now they can see them better," he says.

However, the financial crisis that began late 2008 and intensified during 2009 is prompting many organizations to cut IT budgets, Sapiro explained.

When companies do spend on items such as application security, Sapiro said, the expense is not tied in to application development.

Companies were increasingly outsourcing security rather than look to in-house solutions, the survey found.

Slightly more organizations are willing to outsource (62 per cent in 2009 versus 60 per cent in 2009).

There was a policy shift towards on-shoring or security outsourcing, but over-all security outsourcing continues to grow.

Companies that outsource app development are able to achieve greater security because they are able to compel developers and service providers to include security which meets regulatory standards, Sapiro says.

"Rather than spend time and money on developing security, these companies are paying outsourcers to deliver security that meet Canadian standards."

One security architect, expressed doubts that this model would work for all Canadian organizations.

Managed services, outsourcing of security or databases are often frowned upon by public sector organizations, according to Daria Ribar, an Ottawa-based project manager, security architect and senior security consultant.

"Many of my clients are actually hesitant to have data leave their control or network," she said.

She said organizations considering managed services or outsourcing of app development and IT security need to develop appropriate security polices around the practice.

Eric Marhafer, account executive with Core Security Technologies, a Boston, Mass-based penetration testing software and services company, agrees.

For instance, Marhafer said, hosted app providers often make changes or upgrades to their own applications. In fact it is part of the bargain that MSP clients save money by no longer having to spend on software maintenance and upgrade.

"But clients must be informed about any changes and these clients must test what impact these changes have in their security posture," he said.

Cloud computing

Despite recent media hype of outages suffered by Google's Gmail, companies are less concerned about the reliability of cloud computing services, according to the Telus-Rotmans survey.

In fact cloud computing service availability ranked lowest in concerns of respondents.

IT decision makers were more worried about governance aspects of cloud computing. The top three concerns against using security services in the cloud were:

1. Location of data
2. Connecting business critical systems to security mechanisms outside the business' full control
3. Technical challenges associated with security in multi-tenant environments

Insider threats and malware

The gap between Canada and the U.S. as far as insider breaches are concerned has narrowed considerably.

In 2008, about one in six Canadian companies reported insider activity-related breaches. The number for American companies at that time was close to three out of five.

Related: How to prevent unhappy employees from stealing company data

In 2009, one in three of Canadian organizations reported insider-type breaches compared to the 44 per cent reported by U.S. counterparts for the same period.

You would think that local companies would be spending more on technology detecting and preventing internal abuse, Sapiro says. But that's not the case.

"The footprint of these technologies within Canadian firms actually decreased," he said.

Companies instead spend their IT security budgets on the following technologies:

1. E-mail security
2. Anti-virus
3. Patch management
4. Vulnerability detection and management
5. Content and malware filtering

Sapiro traced the trend to “satisfaction levels.”

Companies, were likely to look favourably at the return of investment in anti-malware products because they have more measurable results, Sapiro said. “You buy them to detect and delete malware and then you can forget about them.”

Insider threat detection technologies are more complex.

“They automate detection but the needed response still require human participation and create pressure on security teams,” Sapiro said.

Print

Close Window