

Security breaches up, but Canadians may be better prepared: study

Information security breaches are up among Canadian organizations, according to an annual [Telus Corp. / Rotman School of Management](#) study – but it's not necessarily all bad news.

In fact, data from the [2009 Rotman-Telus Joint Study on Canadian IT Security Practices](#) suggests that the increase could reflect improved security monitoring and reporting – the result of stronger security mechanisms in response to strict information-protection regulations, according to the report's authors.

Presenting at the [Toronto Board of Trade](#) this week, Dr. Walid Hejazi, a professor of business economics at Rotman, said that the average annual cost of dealing with an information breach nearly doubled from 2008 to 2009, going from \$423,469 last year to \$834,149 in the study of 600 IT security professionals. As well, the average number of breaches per organization increased from three to 11.

The good news? That increase results in part from greater investments in technology and processes designed to help organizations meet new information-governance rules, Hejazi said. Companies are catching more of these infiltration attempts and assigning more money to deal with them.

In an interview after the Board of Trade presentation, Alan Lefort, managing director of Telus's security labs, explained that "breach costs" could include the price of a consultant called in to help an organization avoid future breaches, and technology to thwart infiltrations down the road.

And even though the number of breaches went up, the cost of dealing with individual breaches decreased, because organizations are getting better at responding to the situations, according to the report.

But regulatory compliance and security investments don't account for all of the increases. The study's authors pointed out that the economy plays a role as well.

"As job losses mount, security threats increase," Hejazi said. When organizations lay people off, a certain number of affected employees take company property with them – e-mail lists, documentation on intellectual property, sometimes a laptop.... As well, IT budgets are squeezed these days, making it difficult for IT departments to prioritize spending on security.

Government organizations witnessed the greatest breach-cost increase, jumping from \$321,000 in 2008 to \$1 million this year. Private companies saw their costs increase from \$294,000 to \$807,000. Publicly traded companies saw a relatively small increase of six per cent.

Hejazi said there are a number of reasons for the increase among government organizations: they tend to be targets of breach attempts, because they often manage personal information belonging to citizens, and they often have small workforces not necessarily focused on data security. (Hejazi was also adamant that the real threat for most organizations comes from the inside – not from external hackers.) But "government organizations are performing quite effectively," he said, in terms of paying IT professionals well, involving IT security experts in managing and developing security practices, and aligning processes with those used by large companies.

Organizations that outsourced their IT security operations seemed to fare better than those that didn't, the

study's authors said. Outsourcing enterprises tended to have better IT security protections. They also tended towards "a much more mature" governance model, higher IT security satisfaction ratings, and fewer breaches, Hejazi said.

But governance is the key, he added. Organizations need to have a thorough understanding of exactly which processes they're outsourcing, and a clear picture of just what "success" means in terms of the contract if they want to benefit from an outsourcing agreement, he said.

Indeed, governance, employee education, and executive buy-in might be the most important pieces of the puzzle. "Technology is the last thing we should think about when it comes to security," Lefort said.

For instance, the study found that organizations with more remote workers tended to have fewer information-security breaches. The data showed that these organizations usually trained their staff members harder on protection protocols, perhaps anticipating that the roving workers with mobile access to corporate networks represented a potential vulnerability. "Helping them understand what role they play in security matters immensely," Lefort said.

On hand during the presentation was Christopher Burgess, senior security advisor to the CSO of network technology provider Cisco Systems Inc. (www.cisco.com), and co-author of "Secrets Stolen, Fortunes Lost, Preventing Intellectual Property Theft and Economic Espionage in the 21st Century." In his experience, the threats are changing. Hobbyist hackers are no longer the big concern. "We're not dealing with hackers anymore. We're dealing with people who are as professional as you or I," he said.

Every organization is at risk. "If you have something of value that the criminal element can monetize, you are a target," he said.

As a result, companies need to make sure everyone has information security on their mind. After all, information is usually what sets companies apart – and that differentiation spells a going concern. "Security is how you keep your job," Burgess said.

As well, it pays to keep certain questions about information access in mind: What kind of information is available on the corporate network? How do people access that information? Who is really in control of the information? "Do you control it? Does a third party control it? Or do you not know who controls it?"

Security threats are flexible; security responses need to be flexible too. "Your security footprint will change every day," Burgess said. "This is not a once-and-done."

Lefort echoed that point when he outlined the best practices employed by the top security performers in the study:

- Manage the complete breach cycle: Learn from the experience and change your practices to prevent a similar breach in the future.
- Develop flexible programs based on threats: Let the security team change tactics on the fly; avoid locking them into a response pattern based solely on budget-refresh schedules.
- Educate across the board: Make security a part of everyone's work, from the administrative assistants to the software developers creating new applications.

One major takeaway: the real threat is inside, not outside. Information theft from insiders is more prevalent and damaging than thefts from external hackers, Lefort said.