Security needs to move beyond detection

The good news is that businesses are getting better at detecting security attacks. Now, businesses just have to get better at working to remediate against and prevent those attacks.

“Detection alone is not security,” Ben Sapiro, research director for the security practice at Telus Security Labs , told attendees at the SecTor Security Education Conference Wednesday in Toronto. “A lot of work is being done on finding the problems, but not enough on solving them.”

Sapiro presented his own spin on the recent study on Canadian IT security practices by Telus and the Rottman School of Management, which notes – among other findings – that from last year to this year, businesses discovered almost four times as many breaches, but the cost per breach went down.

Sapiro said this is because companies have become better at discovering when they’re being attacked, largely because of the importance of compliance legislation in both the Canada and the US over the last few years.

“Last year, people were experiencing a similar number of breaches, they just weren’t finding them,” Sapiro said.

But the problem is that many business execs back off their security pushes when “they’ve got all the little checkmarks from their lawyers” that they are able to detect any attempted breaches.

The Telus/Rotman study takes a look at how much companies are spending on security to be happy with their security posture. In the 2008 edition of the study, businesses were happiest when spending five per cent of their overall IT budget on security, that is to say that further investment in security did not equate with further satisfaction in their actual security posture. In 2009, that figure jumped threefold to 15 per cent, largely because of the increasing costs of dealing with all the breaches that are now being discovered.

One of the challenges is that setting up proper systems, services and procedures is an easy-to-predict budget item. Actually dealing with those actual or attempted breaches, though, is a budget wild card. The costs depend on a number of factors, including the nature and severity of the breach.

To help deal with that, Sapiro advocates a hybrid approach to security budgeting, going into a fiscal year with both a core operations budget to handle maintaining security, and a more discretionary budget earmarked for dealing with problems that do arise.

Budgets alone, of course, are not the only factor. “It’s also how you execute on it,” Sapiro said.

And those who are executing well on it are measuring the costs and performance of their security efforts with business-level statistics. Sapiro said that other common threads among those happy with their security efforts include making IT staff, even those not directly responsible for security, accountable for the security efforts of their projects and mandates, and linking compensation and performance measurement to that accountability. And while that may seem a little more “stick” than “carrot,” Sapiro said the number one thing security can do is to build a culture of security through awareness programs.

“Teach them about the benefits of being secure,” he said.

To get through to business leaders, Sapiro said security professionals should focus on the things that are on their mind. And what's on their mind is compliance, a great foot in the door. Behind that, the top-performing categories are all "the boogeyman stuff," as Sapiro put it: fear of security breaches; fear of internal risk; fear of negative media and publicity in the face of a breach.

"Lead with the negative reasons," Sapiro advised.

If that seems a little cynical, there are other routes to get inside business' ear. For example, security professionals can look towards projects viewed as being competitive enablers, and getting security attached to those projects, or at least heavily promoting the importance of security in those efforts.

Don't underestimate the power of specific applications, brought in as business differentiators and competitive advantages, to improve overall security positioning. For example, while at first blush, remote workers and teleworking seems to be a security nightmare because of the disparate users using disparate devices on disparate, and uncontrolled, networks. Still, the report found that organizations that allow more remote access are happier with their overall security posture, largely because more users were educated on the need for security as a condition of having remote access.