itbusiness.ca
Business Advantage through Technology

Print

Selling security without playing the fear card

Users may not always punish companies for security lapses, but that doesn't mean IT can afford to let security slide
11/19/2010 9:01:00 AM
by Shane Schick

The fallout of an IT security breach is sometimes less certain than its cause, but experts almost always describe it in the most dire terms. Shareholders will punish irresponsible companies. Reputations will suffer. Customers, betrayed by the loss of their personal information, will flock to competitors.

Except sometimes they don't.

At last month's SecTor conference in Toronto – the show produced by CMS Consulting's Brian Bourne and others – I sat in on a keynote presentation by Mike Rothman of Securosis in the U.S. His talk, titled "Involuntary Case Studies in Data Security," walked through some infamous and a few lesser-known incidents of organizations that had suffered from poor practices or particularly clever hackers. In one case, however, he produced a disturbingly counter-intuitive factoid.

It was about TJX, the retail giant that operates Winners and Homesense stores here in Canada, and the highly-publicized incident three years ago in which thousands of credit, debit and other transaction information from TJX customers was stolen by hackers. While many observers thought the breach would mean a big hit to the company's business, Rothman showed that sales actually increased at TJX following the lengthy aftermath, compared to the previous year.

What gives? If failing to properly upgrade networks and install the right protection doesn't lead to severe bottom-line consequences, how are resellers supposed to sell security products and services? Certainly after the TJX breach came to light I saw countless PowerPoint presentations from vendors and analysts who used the firm as a cautionary tale in what to avoid. I'm sure many resellers passed along the same kind of horror stories to customers who were reluctant to spend on the latest anti-virus software. Looking around at the new Winners stories in Toronto's financial district, however, it's hard to see any signs of the damage to TJX today.

Rothman had some other good points. "Don't expect people to change – ever," he said, referring to the user behaviours that often lead to security breaches. Not all threats are created equal, he pointed out, which calls for a variety of approaches to protecting information, and "all checklists are wrong." Finally, he said incident response is more important than any single IT security control.

But incident response is determined, in part, by the culture of the organization that will be doing the responding. This is where a true VAR needs to offer some influence and some guidance, and it can't all be based on fear. Security can be an exciting topic because you're sometimes literally dealing with cops and robbers, a high-stakes drama worthy of a John Grisham thriller. Yet the best IT security is often seen as anything but exciting. In fact, if a company hasn't had an attack, it's often that much harder to get them to invest in products and services.

Resellers need to help their customers see security as something that drives business, and not merely something that protects it. A secure organization is less distracted and more efficient. Superior IT security means employees put great value on information that matters to customers. An enterprise with the right security gives staff the courage to take worthwhile risks that lead to breakthrough outcomes. An IT security breach may not bring a company to its knees. But resellers should want to help their clients go far beyond that.

Follow Shane Schick on Twitter: @ShaneSchick.

Print

Close Window