Communications a missing aspect of security: panel

by Robert Dutt

While IT has done a good job of securing communications, it could still do better at communicating security, a panel of security experts said.

Speaking at the Toronto-based SecTor security conference, a group of current and former security managers said one of the biggest challenges faced by security professionals is the ability to communicate just what it is they're offering in terms that businesses understand.

Neil Greenberg, director of information security management at CIBC, put it very succinctly. To get the ear of business leaders, he said, IT needs to be able to answer three questions about any IT project. Does it reduce cost? Does it increase revenue? Does it reduce our risks? And you'd better be able to answer them in elevator pitch form, he said.

PERSPECTIVES

- Green TCO includes everything from cradle to grave
- Biggest enemy of Linux netbooks isn't Windows - it's expectations
- Your data is not growing
- Microsoft OOXML controversy rises again
- More Microsoft Live Search bribery

RESEARCH

- Slowing economy hurting cell phone sales growth
- Network neutrality foes should target 'Joe Six-Byte'
- HTC sees Q3 sales grow 31%
- CERN unveils global grid for particle physics research
- U.S. IT jobs dip 2 per cent as downturn hits

PROFILES

- Sarah Palin e-mail hack suspect indicted
- How inventors always get screwed
- Facebook co-founder to leave for own software startup
- Google exec shines light on Android market
- Nokia CEO Olli-Pekka Kallasvuo details services, Symbian

TEST CENTRE

- Five reasons why the BlackBerry Storm rocks
- Google's 'Mail Goggles' set to be your e-mail wingman
- Green heating, power needed for green IT
- Sony revamps e-book reader, but no wireless
- Nokia brings out iPhone 3G competitor

"If you don't have at least two out of those three, and can't explain it to someone I the line of business in 30 seconds or less, you're dead," he said. "If I can't explain a project to my wife, I'm lost. I'll never have any change of getting that project off the ground and succeeding."

Alan LeFort, director of the security portfolio for Telus Security Solutions, said that while communications around security is not thought of often, it is a factor that is absolutely key in the success of any security project.

"You've got to see what's wrong, you've got to fix it, and you've got to tell people," he said.

LeFort pointed to recent research by Telus and Rotman School of Business that notes that there are huge gaps between the security technologies businesses are implementing, and how happy they are with those technologies. And part of that disconnect is because IT is not managing what users' expectations of security solutions are, and is not very good at communicating the nature of the risks that are being mitigated. Some of the blame goes to issues of compliance, he said, which often mandates installing certain security products, but doesn't provide a clear path for the management and utilization of those products.

David Millier, CEO of security vendor SentryMetrics comes at it from a different viewpoint. Using the example of content management and filtering products used to regulate access to the Internet within an organization, he said there's a significant difference in user acceptance and perception of a solution if the rank and file are consulted on and informed of changing policy ahead of time, versus having changes in policy dictated to them.

"Don't assume the company knows best about what the users need," he said. "Let user's know ahead of time why it's happening and how it will affect them. Put a process in place to manage the exceptions, because you know somebody in marketing is going to need access to certain sites, and the same with sales and other departments."

Dale Tasker, project director for the Ministry of Government Service in Ontario, said it comes back to that reliable old acronym: KISS, or keep it simple, stupid. And the simple message isn't always the same. For base-level users, Tasker advocated using a simple message about how security relates to them, going as far as saying education about how to security their Internet environment at home can make users more aware of the security needs of the business. But that message has to change when you're talking instead to business leaders.

"As you move up the ladder and pitch for dollars to put in products, talk to the value those solutions will bring the organization," he said. "It's all about understanding your stakeholder and your audience."

Christopher Hoff, chief security architect at Unisys, advocated "becoming advisors rather than