
Print

Security admins offer their risk management pitch

Representatives from CIBC, Unisys and elsewhere discuss their approach to selling business leaders on the right products and strategy for protecting enterprise information. Coverage from SecTor 2008

By: Rafael Ruffolo

ComputerWorld Canada (08 Oct 2008)

Managing IT security in the face of your enterprise's political and economic pressures can be a daunting task – but not an impossible one, experts told the Security Conference Toronto (SecTor) on Tuesday.

In a panel discussion that included everyone from CEOs to security architects, executives stressed the need for IT to sell the idea of risk management to the business leaders responsible for funding security projects.

Alan LeFort, director of product management at Telus Security Solutions, said prioritizing and responding to the most pressing security threats your company faces will allow you to conserve valuable time and keep the bosses happy in the process.

"If you can go home at night and say you handled the riskiest things that facing your organization on that day, you've done the best for your company," he said.

Christopher Hoff, chief security architect at Unisys Corp., agreed, saying that instead of trying to patch all 200 servers after Patch Tuesday, security administrators would be better served to re-evaluate where their risk is and tackle those problems from the start. "Taking care of a Severity 5 vulnerability in the print server," he said, is not as effective as dealing with a Severity 2 vulnerability on a front-serving system.

Failing to consider risk has also led to a significant number of companies overspending on the wrong security products and services. Citing results from a recent Telus survey, LeFort said a huge gap exists between the utilization of security products – such as SIEM/Log management, identity management and application security tools – and the satisfaction of these products.

"People are buying this stuff and putting them into place without knowing much about them," he said. "Buying technology to detect vulnerabilities is OK, but what you really should be buying is something that lowers risk." Finding out that you have thousands of vulnerabilities and no time to fix them will not place you in the boss' good books, he added.

The answer, according to Neil Greenberg, director of ESA information security management for the CIBC, has always been to simply follow the money. If your security initiatives are working to reduce costs, increasing revenue, and enabling the business to do something it couldn't before, you're on the right track, he said.

"The business impact is the least thought about piece among security administrators," Greenberg said. "For every project you undertake, you need to have a 30 second elevator pitch. It's really not different than trying to get funding for a start-up business."

According to Jennifer Jabbusch, network security engineer at Siler City, NC.-based Carolina Advanced Digital Inc., finding a way to take advantage of the technology you already have is usually better than buying more expensive security products from a major vendor.

"You can use switches instead of a Network Access Control (NAC)," she said. To monitor your networks, Jabbusch said, using an sFlow instead of a costly intrusion detection system from Q-1 Labs or Norton, may also do the trick.

And in addition to keeping business leaders in the loop, every security decision should also be weighed against its impact on end-users. David Millier, CEO at SentryMetrics, said as more companies restrict Internet access to their users, many security administrators are fielding calls from unhappy users – many of which need to use specific sites throughout the course of their working day.

"You need to put measures in place to find out if there's an effective way to enforce the policies you plan to enact, as well as, a way to monitor whether the policy is actually an effective one," he said. Companies are better off with no policy, as opposed to a false sense of security, Millier added.

Dale Tasker, a former IT security manager with the Government of Ontario, said that along with risk assessment, making sure you're security measures don't overtly conflict with your end-users' ability to function is crucial. Penetration testing before a major application or security project goes live, he said, is a highly valuable best practice.