IN SECURITY, CONSTANT MONITORING COUNTS
Scholl, Frederick
CRN; Oct 18, 2004; 1117; ABI/INFORM Complete
pg. 38

op/ed

REAL VALUES

SOME FRESH AIR

BY HEATHER CLANCY

Things are getting exciting again in infrastructure.

Inspired by what they see as gaps in 3Com's and Cisco Systems' channel programs, D-Link Systems and Juniper Networks are jumping in with both feet. While we need to give their efforts at least six months to see if they'll be successful, both companies clearly have upset the status quo, doubtless prompting soul-searching among their competitors. In particular, both are welcoming their rivals' partners into their own programs with minimal investment on solution providers' parts, especially when it comes to recognizing technical certifications.

This, of course, is a big deal. In *CRN*'s annual solution provider survey on certifications, Cisco certifications routinely show up on the list of the 15 most important designations. More important, three of the top five certifications considered in 2004 to provide the highest ROI for solution providers were Cisco titles.

By recognizing that few solution providers will be willing to simply dump these certifications to risk taking on a new vendor, D-Link and Juniper are removing one of the top objections to their channel program pitches—the time and money it takes to get technical personnel trained.

Moreover, Juniper has honed in on one of the current debates in the channel with respect to Cisco's current program: that its Gold and Silver tiering designations have lost some of their luster as the vendor has shifted to emphasize specializations in advanced technologies such as security or VoIP. Responding to these rumblings, Juniper has focused on the delineation between the top tiers of its own program, hoping to provide ample room for differentiation.

D-Link, for its part, is taking advantage of recent turmoil among 3Com VARs, looking to poach partners cut out of 3Com's top two tiers. D-Link's new Business Solutions Partner Program, set to launch Nov. 1, should provide a clearer line between the vendor's support of resellers focused on SOHO and consumer markets and solution providers with strength in the SMB arena.

Cisco's channel executives are way too smart to ignore these recent developments. I don't know 3Com's team well enough to predict what they'll do. One thing is certain, however: Solution providers will be courted like never before.

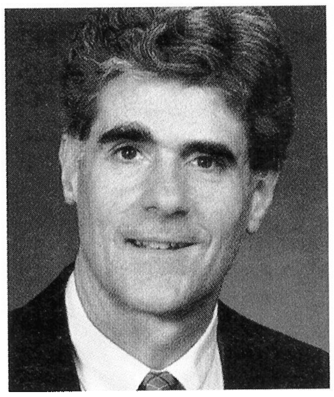
Are Cisco and 3Com vulnerable? Contact HEATHER CLANCY, Editor at *CRN*, at hclancy@cmp.com. Or reach her via AIM at hclancyCRN.

IN SECURITY, CONSTANT MONITORING COUNTS

BY DR. FREDERICK SCHOLL

We seem to live in an age of lawlessness.

At least one-half of the cars I pass on the road are commanded by drivers chatting on cellular phones, in very public violation of New York state law. On another level, news headlines regularly document the indictments, trials and prison sentences involving corporate executives. While large, global firms dominate these headlines, my research and experience indicate that many midsize firms currently are exposed to significant internal security threats that they have not considered.



FREDERICK SCHOLL of Monarch information Networks specializes in Internet forensics and procedures to help clients avoid compliance issues. He is located in Rye, N.Y., and can be reached at freds@monarch-info.com.

Shakespeare's Hamlet may have found one honest man in 10,000, but I find that insider security threats are responsible for about 60 percent of the financial losses prosecuted under the Federal Computer Fraud and Abuse Act. These statistics can be gleaned from www.cybercrime.gov, along with good descriptions of actual computer fraud cases from all sorts of information sources.

Some businesses, like those in the media and entertainment industries, are especially vulnerable to the insider threats. New security requirements mandated by Sarbanes-Oxley and HIPAA legislation will add further risks from internal employees, business partners, contractors and other insiders. The midsize firm isn't typically a target of choice for hackers from outside the company, but it is a target of opportunity for individuals who have inside access and information.

These observations suggest new business opportunities for solution providers interested in supporting midsize companies.

Successful security services should focus on securing total business processes, not simply on securing routers, Web servers and other types of point technologies. A review of each major business process by a security solution provider will inevitably expose existing security holes that need to be addressed and closed.

A secure business process is one that is monitored on a regular basis. Monitoring is called for or implied as a required security control in HIPAA, Sarbanes-Oxley and all other recent security-related legislation. Monitoring goes way beyond simple periodic audits. Businesses today cannot allow problems to continue until the week before quarter- or year-end.

N-able Technologies is one company ahead of the pack in providing tools for solution providers that want to monitor the business processes of their customers. The company's N-central network monitoring offering enables service providers to remotely manage the client's security state, while N-vision is a software solution that the end client can install and use for security monitoring with respect to IT governance policies. The latter is organized around observing key business processes. Both products incorporate N-able's Security Event Manager (SEM), which watches events generated by security platforms that have already been installed within the enterprise. While a number of such tools have been designed for the global corporation, SEM is one of the few designed for the midsize company.

If you're entering the managed security services realm, focus your security services on business processes. Use your understanding of the client to identify likely high-risk areas, and utilize monitoring as a tool to uncover current risks and identify areas for improvement. And, finally, employ tools specifically designed for your market niche.

EDITOR'S NOTE: CRN *welcomes letters and guest commentaries from solution providers. Send your suggestions to* CRN *Editor Heather Clancy at hclancy@cmp.com.*

PHOTO: [Scholl] Courtesy of Monarch Information Networks