CRN Vital Information for VARs and Technology Integrators

September 12, 2003

Network & Security Technologies

NEWS

U.S. Homeland Networks Still A Risky Business

Solution providers continue to see lag in security spending

By Paula Rooney

CRN

- 4:04 PM EST Fri., Sept. 12, 2003

On the two-year anniversary of the 9/11 terrorist attacks, U.S. homeland computer networks remain wide open to attacks by worm and virus writers, cybercriminals and cyberterrorists, solution providers said.

At a *CRN* roundtable discussion in New York last week, top security solution providers said that while businesses invested in disaster-recovery software immediately after the terrorist attacks, overall adoption of security technologies has changed little.

And they said the Department of Homeland Security so far has not dug into its pockets to better secure government networks.

Physical security at U.S. airports has improved dramatically, but IT security has not, said Adam Lipson, president and CEO of Network & Security Technologies, Pearl River, N.Y.

>> Despite investments in disaster recovery after 9/11, adoption of security technologies is slow

"The U.S. government has continued spending money on traditional security tools including intrusion-detection systems, firewall technology and virus and patch management systems, but I believe the spending that's occurring is more of a steady state than a result of the 9/11 tragedy," he said.

Added Gary Morse, president of Razorpoint Security Technologies, New York: "I see very little change [in security spending] since 9/11. So many networks are so wide open."

Gene Hodges, president of Network Associates, Santa Clara, Calif., noted: "There was going to be this huge tidal wave of money around homeland security. That hasn't happened. There's been a lot more hype than real cash from the government."

Meanwhile, the cost of hacker activity is on the rise. Industry trade group CompTIA said cybersecurity breaches cost businesses in excess of $13 billion in 2002 and will rise in 2003.

The MSBlaster and Sobig.F worms this summer underscored gaping security holes across the nation's computer infrastructure. Last week, Microsoft issued yet another fix to shield three more "critical" vulnerabilities in Windows that could allow hackers to take control of desktop PCs and servers.

And concerns about cyberterrorism are not unfounded, solution providers added. "The issue continues to be the perceived lack of interest and capability of traditional terrorist groups to exploit this attack vector," Lipson said.