



September 11, 2003



On Second Anniversary of 9/11, Computer Security On U.S. Homeland Is Lax

Experts say businesses wide open for attack

By [Paula Rooney](#)

CRN

- 12:25 PM EST Thurs., Sept. 11, 2003

Experts say that today, on the two-year anniversary of 9/11, U.S. homeland computer networks remain wide open to attacks by worm and virus writers, cybercriminals and cyberterrorists. The Department of Homeland Security, they add, has made little progress securing government and corporate networks.

At a *CRN* roundtable discussion on IT security in New York Tuesday, top security solution providers said that while businesses invested in disaster-recovery software immediately after the terrorist attacks, most have spent little money securing their desktops and servers, and even less on network security assessments for their infrastructures.

While physical security in the United States has changed dramatically, IT security has changed only modestly, said Adam Lipson, president and CEO of Network & Security Technologies, an IT security consulting firm in Pearl River, N.Y., that participated in *CRN*'s security roundtable discussion. "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."

Added Gary Morse, president of New York-based RazorPoint Security Technologies and another roundtable participant: "I see very little change since 9/11. "So many networks are so wide open."

Recent security breaches, this summer's Blaster and Sobig.F worms, for example, served to underscore IT security vulnerabilities in this country, solution providers said.

Microsoft, whose Windows operating system remains a chief target for hackers, issued yet another fix on Wednesday to shield three more "critical" vulnerabilities that could be exploited to infiltrate the PCs of millions of users worldwide.

While many solution providers consider Windows particularly susceptible to hacker attack, Unix and Linux are not foolproof either, Morse said.

Late last month, for instance, The SCO Group's Web site was shut down for a weekend after an attack by hackers that were reportedly irate about the company's multibillion-dollar lawsuit against IBM.

Meanwhile, the cost of U.S. hacker activity continues to rise. According to information submitted to the U.S. government this week by industry trade group CompTIA, the economic impact of cybersecurity breaches in 2002 exceeded \$13 billion and will rise in 2003.

While the past few months have been difficult, federal and local law enforcement agencies have made significant progress arresting alleged hackers and worm writers, solution providers said.

Late last week, federal authorities nabbed an 18-year-old Minnesota teen charged with distributing a variant of the Blaster worm that caused major corporate headaches this summer. On Wednesday, a 24-year-old Romanian man caught last week was officially charged with cybercrime offenses that carry a punishment of up to 15 years in prison, Romanian police said.

Solution providers also say they're encouraged that Microsoft is doing a better job of educating the public about prevention and publicizing ways that users can easily inoculate their systems and networks by downloading patches and fixes from Windows Update.

Even so, the costs for handling the outbreaks are increasing. According to Central Command, an antivirus software company, August 2003 was the worst month for computer viruses in history.

"The past 30 days have been particularly harsh for many owners and users of IT," said Oli Thordarson, president of Alvaka Networks, Huntington Beach, Calif. "The Sobig.F and Blaster worms have wreaked havoc on those who left themselves vulnerable. Certainly, clients who have adopted the practice of protection have fared the best. These folks have avoided big unexpected costs, embarrassment and loss of revenues. The biggest problem clients are facing today is timely deployment of patches on PCs and servers. A single patch typically costs between \$50 and \$100 per system when you factor in costs of technical personnel. Even harder to compute, but vastly more expensive, is the cost of not deploying patches."

And the vulnerabilities in Windows are the least of the problems, solution providers say.

The less publicized yet more heinous offenses perpetrated by professional cybercriminals and potential cyberterrorists pose a far more serious threat to the security of commerce and government activities, said security solution providers at *CRN's* roundtable.

Morse noted, for instance, that several large financial institutions have been outright robbed while other hackers have commandeered private business servers and used them to distribute MP3 files and videos illegally.

This week, a 22-year-old known as "the homeless hacker" turned himself in at a federal courthouse in Sacramento, Calif., after a federal warrant was issued for his arrest. The man is charged with breaking into *The New York Times'* databases during a period of three months in 2002 and causing damages exceeding \$25,000.

"The bottom line is that, yes, government and commercial systems are vulnerable to electronic attack, and each new vulnerability and worm reinforces that," said Lipson. "The issue continues to be the perceived lack of interest and capability of traditional terrorist groups to exploit this attack vector."

The Congressional Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census held a hearing this week to discuss the cybersecurity of businesses and governmental agencies.

At the hearing in Washington on Wednesday, CompTIA said change must come from the highest levels of the U.S. government.

According to testimony submitted to the committee by CompTIA, the government's "IT vulnerabilities are well-documented," and the group urged the federal government to take a more active role in preventing cybersecurity breaches.

"The federal government must lead by example," wrote Tom Santaniello, manager of U.S. Public Policy at CompTIA. "The federal government must first commit to a total cybersecurity solution before asking the private sector for such a commitment. Committing to cybersecurity will require a total commitment not only to hardware and software but also to training and certification."

According to the industry association, the Computer Emergency Response Team Coordination Center (CERT/CC) operated by Carnegie Mellon University handled 82,000 computer security breaches in 2002, up substantially from 22,000 incidents in the prior year.

Many solution providers serving the U.S. government and businesses maintain that the Department of Homeland Security has been slow to take action aimed at preventing cybercrime and potential cyberterrorism.

But while the wheels of bureaucracy grind slowly, the U.S. government and Department of Homeland Security are doing network assessments, establishing standards and developing a secure network infrastructure that businesses and governmental agencies can rely on in the future.

"They're spending a ton of money on homeland security," said one security VAR, who requested anonymity. "We haven't seen any contracts, but they're coming."

1NService Company, a coalition of 16 solution providers serving the U.S. government's security IT needs, said it expects government spending to explode over the next two years. Ten of those solution providers are working directly with the Department of Homeland Security.

"Unfortunately, there's a catch-22 in funding. It's a challenge for the government. It takes a long time [for the security infrastructure] to be deployed, and it's not going to happen overnight," said Dave Austin, vice president and general manager of SmartNet, a security solution provider and 1NService member. "But they're making good progress. There's been a significant across-the-board commitment to upgrade systems from network security to voice to physical security."

On the other hand, software and hardware vendors that expected to see big business from the government after the terrorist attacks are disappointed.

"The commercial accounts are spending more, but the government spending has been really hyped," said Gene Hodges, president of Network Associates. "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, I think, from the government."