

FCW.COM



Panel must narrow cybersecurity scope

31 experts form a commission to give next president their advice on network defenses

By Jason Miller

Published on November 5, 2007

A new blue-ribbon panel that will develop cybersecurity recommendations for the next president faces a compressed schedule and the challenge of agreeing on a cybersecurity agenda that it wants the next administration to address.

Experts say cyberthreats from terrorists, organized crime and other countries lack a common thread and instead stem from a variety of vulnerabilities, including insufficient training, technology weaknesses and a culture of Internet use that puts the public and private sector at risk. For those reasons, the most obvious recommendation for improving basic cyberdefenses is the hardest to accomplish, said Glenn Schlarman, former branch chief at the Office of Information Policy and Technology at the Office of Management and Budget.

The Center for Strategic and International Studies (CSIS) organized the Commission on Cyber Security for the 44th Presidency and outlined its objectives at an Oct. 31 briefing.

"We want to give the next administration new ideas or policies that they can pick up and run with," said Jim Lewis, director of CSIS' technology and public policy program. "This is a threat that is growing and putting our critical infrastructure and financial systems in peril. People are attacking the U.S. in better and smarter ways, and we need to become better and smarter to deal with them."

Some experts maintain that security measures should address widespread problems.

Schlarman said "nearly every example of something bad that happened — even the Chinese having their way with defense systems — has not been rocket science but poor security practices. We still do not correct commonly known vulnerabilities in information systems. The problem is poor hygiene. There is not some new dirt that we have to get out."

Schlarman and some other experts who are not on the panel said they support its goals, but they said the panel should narrow its scope to be effective.

ADVERTISEMENT

"When you think about information security, there are three main areas to look at: prevention, detection and response," said Daniel Castro, senior analyst at the Information Technology and Innovation Foundation. "Right now, it is not very clear that the U.S. is doing any of these very well."

CSIS named Reps. Jim Langevin (D-R.I.) and Mike McCaul (R-Texas), chairman and ranking member, respectively, of the Homeland Security Committee's Emerging Threats, Cybersecurity, and Science and Technology Subcommittee, as co-chairmen. Scott Charney, vice president at Microsoft's Trustworthy Computing Group, and retired Navy Adm. Bobby Inman, a professor of national policy at the University of Texas at Austin, will represent industry as the panel's co-chairmen.

The 31-member commission, which includes former federal officials and industry leaders, will hold five plenary sessions to discuss an agenda. The first one is scheduled for this week. The panel plans to submit recommendations to the next president by December 2008, Langevin said.

The commission will offer a blueprint for securing cyberspace, Langevin said. "My philosophy as subcommittee chairman is that we are such a free and open society that it is very difficult if not impossible to secure the Internet. My objective is to identify the most severe vulnerabilities and close them."

Larry Clinton, president at the Internet Security Alliance, said the commission's goals are laudable, but he questioned how it will come up with concrete recommendations in such a short time.

"This is the latest in a series of groups trying to do this," Clinton said, referring to the Partnership for Critical Infrastructure Security, which for the past six years has been trying to coordinate cross-sector initiatives to safeguard critical infrastructure services. "This isn't easy because, if it was, it would have been done. They have a very ambitious schedule."

Lewis said the commission will benefit from its members' familiarity with one another and with the challenges.

"We want to agree on a set of principles that will guide our recommendations," said Bruce McConnell, president at McConnell International and a member of the panel. "That will help us on a lot of the specifics," such as assessing current and future threats, reviewing authorities and policies, and evaluating requirements for critical infrastructure protection.

The commission also will tackle software assurance and ongoing security initiatives in the private and public sectors.

"Since Sept. 11, 2001, the focus has been on physical security threats and we have paid little attention to cyberthreats," McCaul said. "A digital Pearl Harbor [could be] a reality."

Langevin added that the next administration would be unwise to ignore the commission's recommendations.

"There is an opportunity when a new administration comes in, and that is our hope," Lewis said. "The threat is growing, and we have to figure out how we organize ourselves to deal with it."



Simplify your agency's data security with HP reliability.

HP Compaq t5135
VIA Eden 400 MHz
HP ThinConnect
\$285

REPLAY [Learn more »](#)