View From the White House: Fix Vulnerabilities Immediately

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

One of the most interesting lectures at the Sixth National Colloquium on Information Systems Security Education (see http://www.ncisse.org) in Seattle (3-6 June 2002) was a speech by Dick Clarke, the Special Advisor to the President for Cyberspace Security. He stated that cyberspace security would depend primarily on the private sector and that academia will play a vital role in raising the level of security in the United States both in research and in education.

Mr. Richard A. Clarke began his federal service in 1973 in the Office of the Secretary of Defense as an analyst on nuclear weapons and European security issues. On October 9, 2001, he was appointed Special Advisor to the President for Cyberspace Security <http://www.whitehouse.gov/news/releases/2001/10/20011009-4.html>; as such, he coordinates interagency efforts to secure information systems, particularly in the event of a disruption, when must coordinate efforts to restore critical systems. He strongly supports the private sector, which owns and operates the vast majority of America's critical infrastructure.

Mr Clarke said that this year has seen many changes in security thinking. After the events of September, security rose to top priority in everyone’s mind; however, he opposes the use of the word “cyberterrorism” because it suggests that known terrorist groups will use information warfare techniques against us. But this is a limitation in our thinking according to Clarke: we have never seen a terrorist group apply information warfare against us. They use it for communications and recruitment, but never for direct attacks. In any case, it doesn’t matter who’s causing damage to our information infrastructure. We’re never going to be able to tell people in advance on a consistent basis who’s going to attack what, when and how, so let’s worry about the vulnerabilities, not the threats. Mr Clarke asserted that private sector organizations don’t need to wait for the intelligence services to find the attackers. Do your vulnerability analysis, rank the vulnerabilities, and start solving the problems step by step. Said Clarke, “The problem is yours, not ours. It’s a problem where law enforcement, the military and the government cannot secure your systems. We’re never going to allow the FBI or the US Army to tell a bank how to configure their networks.”

As for US federal government efforts, after 9/11 agencies examined the vulnerability assessments for a number of agencies and discovered that many of them were _not_ planning for remediation. The requests were sent back to the agencies and the result of the new focus was a 64% increase in IT security spending – a $4.5B increase in the budget. So there’s going to be a significant spike in security spending this fall as the budgets move through the process.

* * *

In the next article, I’ll report on Mr Clarke’s comments about the role of higher education in national information assurance.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@compuserve.com>. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at <http://www.mekabay.com/index.htm> for papers and course materials on information technology, security and management.

Copyright © 2002 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.