



A Challenge from Washington

by: Richard Clarke

Pages: C-23; November, 2000

文章简介：本文阐述了信息系统安全对国家安全的重要性，提出了各机构应该遵循的七项信息系统安全原则。本文作者是克林顿任命的安全、基础设施保护和反恐的国家首席协调人。



[华安信达](http://ChinaCISSP.com)

National Security Council

Washington, D.C. 20504

October 13, 2000

Andy Hagg

Editor, *Contingency Planning and Management* magazine

Witter Publishing Company

84 Park Avenue

Flemington, NJ 08822

Subject: America's Cyber Security is Everyone's Business



The information technology revolution that has fueled the tremendous growth in our economy has also made us more vulnerable to cyber attack. Major sectors of our economy—finance, telecommunications, energy, transportation and health—rely on information systems. A few malicious keystrokes could seriously disrupt whole sectors of our economy or your business unless prudent defense measures are implemented and regularly updated. Unlike traditional military threats, the Federal government alone cannot defend you from attack. Securing our critical infrastructure is everyone's business.

The Federal government has joined in partnership with over 160 private firms to help secure our information systems. The finance industry has led the way by forming a center to share information related to cyber attacks. Other sectors are forming information sharing centers, but more must be done. Senior management must continue to focus on information systems security. There are no silver bullets. Prudent defense requires implementing technical patches to help prevent attacks and sound company policies and best practices to govern information systems administration.

Private firms must also join together to share information relating to cyber threats and attacks. In September the White House sponsored a "B2B" cyber security conference to facilitate such cooperation among "B2B" leaders.

When considering procurement of new technology, such as wireless communications, business leaders should ask tough questions about the security features or vulnerabilities of new systems.

Finally, I urge business leaders to keep in mind the following seven cyber security principles:

- Designate an individual responsible for information security.
- Identify critical business operations and the degree they depend upon information systems.
- Identify vulnerabilities in critical information systems.
- Demand rigorous security features from information technology suppliers.
- Implement strict information security procedures for all employees.
- Regularly review critical operations, information system vulnerabilities and security procedures
- Establish relationships with peers, vendors, and customers to share information about cyber threats, incidents, and responses.

Sincerely,

Richard A. Clarke

National Coordinator for Security, Infrastructure Protection and
Counter-Terrorism

About Richard A. Clark

President Clinton appointed Richard Clarke as the first National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism in May 1998.

Clarke is a career member of the Senior Executive Service, having begun his federal service in 1973 in the Office of the Secretary of Defense. In the Reagan Administration, he was the Deputy Assistant Secretary of State for Intelligence. In the Bush Administration, he was the Assistant Secretary of State for Politico-Military Affairs. In that capacity, he coordinated State Department support of Desert Storm and led efforts to create post-war security architecture. In 1992, Mr. Clarke joined the National Security Council staff.

Among the issues he has handled, he leads U.S. government efforts on cyber security, counter-terrorism, and domestic preparedness for weapons of mass destruction.

Mr. Clarke is a graduate of the Boston Latin School, the University of Pennsylvania, and the Massachusetts Institute of Technology.