FT-18-2818
John Pescatore, Richard Hunter,
French Caldwell, Richard Stiennon

Gartner FirstTake
18 September 2002

U.S. Cybersecurity Strategy Follows Best Practices

Gartner believes the U.S. National Strategy to Secure Cyberspace takes a sound approach. Enterprises should cooperate immediately, or government regulators may force more intrusive approaches.

Event: On 18 September 2002, the administration of U.S. President George Bush issued a draft of its National Strategy to Secure Cyberspace, which aims to protect national infrastructure from cyber- or physical attacks on the IT systems that support it. The plan will involve:

- Ordinary Internet users
- IT vendors
- Internet service providers and Internet backbone providers
- Enterprises, especially in key industries such as telecommunications, energy and financial services
- Federal, state and local governments
- The international community

The plan sets out a wide array of tasks for these constituencies, ranging from awareness training to national projects, such as a proposal for private industry to cooperate in building a network operations center for the United States.

First Take: Gartner believes the overall approach — avoiding government mandates and regulations — and the general direction of the recommendations follow best practices that have evolved among early adopters of stringent cybersecurity practices. Although security vendors will decry the lack of mandates since many hoped that regulations would spur additional spending on security, the strategy recognizes the realities of business and the power of the market to improve security. Thus, the strategy follows the proven approach of encouraging industry to regulate itself before the government interferes with market mechanisms.

The strategy makes many useful proposals, such as developing a national certification program for IT security professionals and devising ways to protect Supervisory Control and Data Acquisition (SCADA) systems, which govern the power grid.

However, the plan delves into too much detail in some areas (such as wireless LANs) and stays too general in many others (for example, how the national law enforcement and intelligence communities will

define national attacks). The plan also contains significant gaps among the specific proposals. For example, the strategy does not detail how it will implement Presidential Decision Directive 63, issued in May 1998, which places special emphasis on protecting the government's critical assets from cyberattack. The federal government will dramatically increase spending on information security in fiscal 2003, but the plan contains no strategy to ensure that spending leads to better security for the U.S. government, a critical infrastructure segment. The administration has made progress toward this goal by increasing the Office of Management and Budget's power to review IT spending, but it needs to take a more proactive approach to demonstrate leadership. The government can also define security standards and use its buying power to make those standards meaningful in the market.

Gartner offers the following recommendations:

- To create an effective strategy, the planners should prioritize the 24 strategic goals and 86 recommendations.

- Federal, state and local governments should make improving their own security their top priority. Additional spending on security from these sources will demonstrate strong leadership and provide a model for others.

- Enterprises' boards of directors should make information security a high priority. Oversight by the board can be one of the most effective mechanisms for improving enterprise cybersecurity.

- Enterprises should adopt this voluntary approach immediately, or government regulators may force more intrusive approaches.

Enterprises in critical infrastructure segments, particularly energy, transportation, telecommunications and government, should map their information security plans against these guidelines. Otherwise, the cost of implementing mandated solutions will greatly exceed business-driven security improvements. As it updates this strategy, the Critical Infrastructure Protection Board should develop a time frame for progress that will determine when legislation or regulation would be required.

Analytical Sources: Richard Hunter, John Pescatore, Richard Stiennon and French Caldwell, Gartner Research

Recommended Reading and Related Research

- "Toward a National Cybersecurity Strategy" — If it takes a slow, hierarchical approach to developing a national cybersecurity strategy, the U.S. government will impede the market's innate ability to evolve the level of security required to serve U.S. economic interests. **By John Pescatore**

- "'Digital Pearl Harbor' War Game Explores 'Cyberterrorism'" — The United States lacks the ability to assimilate and analyze early warnings of an impending attack and to respond in real time. **By Richard Hunter, John Bace and French Caldwell**

(You may need to sign in or be a Gartner client to access all of this content.)