



COMPUTERWORLD

[Home](#) [News](#) [Topics](#) [Departments](#) [Services](#) [Subscriptions](#) [Events](#)

You may retrieve this story by entering QuickLink# 32669

[Return to story](#)

Corporate America now on front lines of war on terror

By [DAN VERTON](#)
SEPTEMBER 09, 2002

A year ago this week, America was attacked by a global enemy that has demonstrated its determination to use any means at its disposal to wreak havoc and fear, damage the economy and compel the nation to withdraw from the international community ([see story](#)).

In that regard, Sept. 11, 2001, will be remembered as a colossal failure for international terrorism, say government and private-sector security experts.

Dell server consolidation
Saves money.

Dell | Enterprise

The advertisement features a large blue curved shape on the left containing the text 'Dell server consolidation Saves money.' To the right is a black and white photo of a man standing next to a tall Dell server rack. The Dell logo and 'Enterprise' are at the bottom right.

SEPTEMBER 11
IT Responds
View more on this
Special Report

Rather than leaving the country in a state of stunned inaction, the attacks triggered what many security experts say was long overdue: a nationwide effort to bolster homeland security and critical infrastructure protection—a concept that has placed private companies on the front lines of national defense.

"It's never been done before," said Steve Cooper, CIO at the White House's Office of Homeland Security, referring to the massive integration effort now under way to help improve security information sharing among government agencies and the hundreds of private companies that own and operate 90% of the nation's critical systems. "We must do it, and we can do it," said Cooper, speaking Aug. 19 at a government symposium on homeland security.

Perception Game

However, proponents of critical-infrastructure protection, particularly in the area of cybersecurity, face many of the same challenges that terrorism experts encountered prior to Sept. 11: Few in the private sector perceive that there's an imminent threat to the digital homeland, and fewer still acknowledge terrorists' ability to and willingness to adapt their tactics to take advantage of America's digital Achilles' heel—its information networks.

Every so-called critical infrastructure in the U.S., from telecommunications to transportation, banking and energy, relies on computers and computer networks, National Security Adviser Condoleezza Rice said in March last year during her first major policy address on the topic ([see story](#)).

"Corrupt those networks, and you disrupt this nation," she said. "Today, the cybereconomy is the economy."

"The terrorists in the Sept. 11 event had the patience to plan [and] the foresight and the understanding of the infrastructure that could be used to simultaneously or sequentially disrupt the infrastructure electronically," said Paula Scalingi, former director of critical infrastructure protection at the U.S. Department of Energy. "That could cause a major regional failure in this country. There's no question that that's doable."

Game of Dominoes

The reality of the threat to the nation's critical infrastructure, particularly in the areas of power, telecommunications and emergency services, was demonstrated in June when the federal government co-sponsored an exercise known as Blue Cascades. Dozens of government and private-sector representatives from five U.S. states in the Pacific Northwest and three Canadian provinces confronted the very real potential for cascading infrastructure failures resulting from combined physical and cyberterrorist incidents.

The results were chilling ([see story](#)). Simulated terrorist attacks disrupted the region's electric power grid, causing power outages that spread quickly to other Western states and lasted for more than a week, according to exercise coordinators. The exercise also included simultaneous physical and cyberdisruptions of the region's telecommunications and natural gas distribution systems, as well as a threat to a major municipal water system and the region's ports.

Once the electric grid is disrupted, the other infrastructures that businesses and government agencies rely on for their day-to-day operations, including telecommunications, transportation, emergency services, hospitals and law enforcement, begin to fall like dominoes, according to the final report on the lessons learned from the exercise.

A year after the Sept. 11 terrorist attacks, has anything changed? What has your company done to better protect its assets? Should the government get more

involved in preventing a cyber 9/11 in the future? Have your say in our Computerworld forum, [9/11 One year later](#).

What Is Critical Infrastructure?

Facilities and IT systems that operate and manage daily services in the following sectors are considered part of the critical infrastructure:

■ Banking and finance

■ Emergency services

■ Energy

■ Essential government services

■ Health care

■ Telecommunications

■ Transportation

■ Water systems

ATTACK ON AMERICA

Recent Headlines

- [Cyberthreats Not to Be Dismissed, Warns Clarke](#)
- [Cyberthreats not to be dismissed, warns Clarke](#)
- [Think tank: Cyberthreat overrated](#)
- [Around the Web](#)

Additional Coverage

- [View our Attack on America special coverage page](#)

Computerworld's continuing coverage of the September 11 attack on America and its aftermath.

Source: Computerworld

Sponsored Links

Prove the Business Value of IT! Attend Computerworld's Premier 100 IT Leaders Conference, Feb 23-25 in Scottsdale!

Free Trial The Advisory Council, practical peer advice for solving IT problems

Learn how to receive a Cisco router valued at \$3,500

[About Us](#) [Contacts](#) [Editorial Calendar](#) [Help Desk](#) [Advertise](#) [Privacy Policy](#)

Find IT solutions fast.

Copyright © 2003 Computerworld Inc. All rights reserved. Reproduction in whole or in part in any form or medium without express [written permission](#) of Computerworld Inc. is prohibited. Computerworld and Computerworld.com and the respective logos are trademarks of International Data Group Inc.