



see for yourself
» [free trial of](#)
[server management software](#)



COMPUTERWORLD

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

You may retrieve this story by entering QuickLink# 31490

► [Return to story](#)

Final 'Blue Cascades' report cites infrastructure gaps

By [DAN VERTON](#)
JULY 18, 2002

Government agencies and the private sector should work together to respond to any coordinated physical and cyberattacks against critical infrastructure systems, a report out today said.

The report follows a high-level exercise last month called Blue Cascades that was sponsored by the Pacific Northwest Economic Region (PNWER). The exercise, the first regional, cross-border event held in North America, showed how entire regions can be to vulnerable to power outages and telecommunications failures ([see story](#)).

The Seattle-based organization includes the states of Alaska, Idaho, Montana, Oregon and Washington, as well as U.S. and Canadian government agencies.

Today's recommendations are from the PNWER's Partnership for Regional Infrastructure Security, which includes those five states and three Canadian provinces and is aimed at outlining how government and the private sector should respond to coordinated physical and cyberattacks.

Participants in Blue Cascades included federal and state officials as well as companies such as The Boeing Co., Pacific Gas & Electric Co., Verizon Communications and Qwest Communications International Inc. The exercise

Click now to
find out more
about a free
ROI analysis.

Flexible solutions that can cut costs today and tomorrow.

Intel Xeon

Easy as DELL™

focused on linkages between infrastructures that could make the Pacific Northwest vulnerable to cascading effects in the event of an attack or disruption that could complicate quick response and recovery.

The critical infrastructures studied in the exercise included energy (electric power, oil and natural gas), telecommunications, transportation, water supply systems, banking and finance, emergency services and government services.

"Our infrastructures follow economic watersheds, which pay little attention to political and jurisdictional boundaries," Rep. Jeff Morris said in a statement. "Our largest vulnerability is how interconnected we are and how little we communicate across these boundaries." Morris is chairman of the Technology, Telecommunications and Energy Committee of the Washington Legislature.

The PNWER report calls for better understanding of the interdependencies among the region's critical infrastructures, development of a regional threat assessment approach and development of ways to enhance communication and coordination among emergency management agencies and industry officials on both sides of the U.S./Canadian border.

It also found fault with the existing color-coded terrorism alert system put in place by the White House's Office of Homeland Security, concluding that it "appeared to be little-understood and conflicted with infrastructure-sector threat levels."

Terrorist attacks directed at disrupting the region's electric power could cause regionwide power outages that spread quickly to other Western states, the report said. It also envisioned follow-on disruptions to the region's telecommunications and natural gas distribution systems, as well as a threat to a major municipal water system and to the region's ports.

The attacks and disruptions of critical services and related response and recovery actions affected other important operations and facilities, including transportation, emergency services and hospitals, medical care and law enforcement.

According to the report, participants in the exercise "demonstrated at best a surface-level understanding of interdependencies and little knowledge of the critical assets of other infrastructures, vulnerabilities and operational dynamics of these regional interconnections, particularly during longer-term disruptions."

In addition, the report said the exercise showed that most companies and government officials failed to recognize their own "overwhelming dependency upon IT-related resources to continue business operations and execute recovery plans."

The report also concluded that law enforcement agencies lack an effective way of getting and sharing threat-related information from the private sector and utilities.

"Preparedness has to be on a regional basis, involving all key stakeholders in a cooperative effort that is based on trust and sharing of relevant information in a secure manner," said Paula Scalingi, former director of critical infrastructure at the U.S. Department of Energy and now a private consultant.

"Sept. 11 demonstrated that U.S. intelligence cannot provide the necessary alert and warning to prevent terrorists from striking," Scalingi said. "What is needed is to improve regional preparedness to deal with the unthinkable."

Source: Computerworld

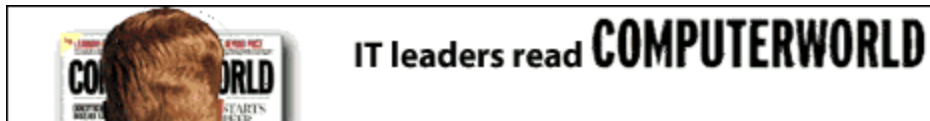
Sponsored Links

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](#)



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.