

'Digital Pearl Harbor': Defending Your Critical Infrastructure

French Caldwell, Richard Hunter

Gartner and the U.S. Naval War College held a war game to examine scenarios for cyberattacks on national critical infrastructure. Participants came away with a vivid sense of what cyberterrorism could do.

ANALYSIS

In July 2002, Gartner and the U.S. Naval War College hosted a three-day, seminar-style war game called "Digital Pearl Harbor" (DPH). Gartner analysts and national security strategists gathered in Newport, Rhode Island, with business and IT leaders from enterprises that control parts of the national critical infrastructure. Our objective was to develop a scenario for a coordinated, cross-industry cyberterrorism event.

Results of a post-game survey indicate that the DPH game experience had a profound impact on the participants: *79 percent of the gamers said that a strategic cyberattack is likely within the next two years.*

DPH participants played the roles of terrorists, devising coordinated attacks against four national critical infrastructure areas: the electrical power grid, financial service systems, telecommunications and the Internet. Their goal was to determine if a cyberattack could create a crisis of confidence that would shift the strategic balance of power, at least temporarily. Since the game did not test defenses against cyberterrorism, the questions of whether a real attack would achieve the goals set in the game and how much economic damage it would cause are still open.

The question as to whether cyberterrorism is a realistic threat *is* resolved. DPH skeptics abound, of course, and level many criticisms, but two criticisms stand out.

The first criticism is that by engaging in this type of exercise, we are opening Pandora's box, showing those with malicious intent what could be done. Good point, but before we started, we ran this issue by national security officials, and as one of those officials succinctly put it: "The bad guys already have the knowledge of these systems, and they know what they are going to do." The purpose of the DPH game was to get inside the opponents' heads. All of the data and information created in the DPH game underwent a national security review before we published our analyses.

The second criticism is that there are no new lessons to be learned from the DPH game. Good point, and really a very daunting criticism. Yet, how often do we hear from these same critics: "If only enterprises (or users) would follow good IT security practices ..." But good practices are very difficult to follow. How many readers have ever installed a new operating system or application on their home PC, only to spend the next several days trying to get the PC to work again? Multiply that experience by thousands when you are talking about enterprises installing new applications, security patches and system connections on hundreds or thousands of servers, mainframes and PCs. Preventing such downtime requires deliberate, linear steps that take time, people and money. DPH-type exercises help identify the threats, improve risk management processes and, in turn, prioritize resources for IT security activities. As one military commander put it: "We must shoot the closest wolf first."

Nevertheless, the skeptics have history on their side (as do all Luddites at the dawn of a new era) — there has never been a cyberterrorism event. Or has there? Electrical power grid failures in some parts of the world, such as Western India, are so common that tampering with the grid to test cyberattacks could go unnoticed. This path leads to conspiracy theory oblivion, which is one of the reasons we ran the DPH game: determine what is really possible by a cyberattack.

Even skeptics of a DPH-type attack must acknowledge that our enterprises are under small-scale cyberattacks every day; hence, we are confident most readers will find our analyses of the DPH war game at least somewhat useful and very interesting.

Featured Research

"Digital Pearl Harbor' War Game Explores 'Cyberterrorism'" By French Caldwell, Richard Hunter and John Bace

"Security Best Practices Will Do Most to Foil Cyberterrorists" By Paul Schmitz, John Mazur and Rich Mogull

"Cyberterror Poses Growing Threat to Financial Services" By John Bace, Annemarie Earley, Vincent Oliva and David Furlonger

"Utilities Should Upgrade the Security of Their Operations" By John Dubiel, Kristian Steenstrup and Paul Pechersky

"Prepare for Cyberattacks on the Power Grid" By John Dubiel, Kristian Steenstrup and Paul Pechersky

"Telecom Is Secure but Not a Cause for Complacency" By David Fraley and Ron Cowles

"Could Terrorists Bring Down the Public Switched Telephone Network?" By David Fraley and Ron Cowles

Recommended Reading and Related Research

"Force Vendors to Make Software More Secure" By Arabella Hallawell and Rich Mogull

"Cyberattacks and Cyberterrorism: What Private Business Must Know"
(www.gartner.com/qa/qa-0902-0091.asp) By Rich Mogull and Richard Hunter

"Dealing With Cyberterrorism: A Primer for Financial Services" (www.gartner.com/qa/qa-1002-0104.asp) By David Furlonger

"Terrorists Could Hijack the Internet" By Ron Cowles and John Mazur

French Caldwell

Editor in Chief

Business and Public Policy

spotlight.feedback@gartner.com

Richard Hunter

Contributing Editor

Business and Public Policy

spotlight.feedback@gartner.com

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509