

Electronic and Human Communication: Engaging the Private Sector in Global Critical Infrastructure Protection

19 September 2006
Georgia Tech Information Security Center

Dr. Phyllis A. Schneck
Vice President, Research Integration
Secure Computing, Inc.
Chairman, Board of Directors,
InfraGard National Members Alliance

"Cyber" and communications system form the nexus of all of our critical infrastructures and key resources: this talk will focus on global protection of critical infrastructures and key resources, from the perspective of cyber as a common thread and one of many interdependencies.

This talk presents the challenges and solutions in securing global systems which maintain our infrastructures such as water, transportation, energy and agriculture. Necessary to protect critical infrastructure is the ability to channel subject matter expertise to share knowledge between corporations, government and law enforcement.

"Information sharing" is a phrase often used and a task seldom accomplished. True information sharing is the result of a trusted relationship. Valuable information sharing brings subject matter expertise across sectors, levels of government, and communities, transcending competition through the power of trust.

By way of example, most recently notorious in the world of phishing and online fraud, is the ability for government and law enforcement to work with private corporations to better understand the landscape and data that normally only the private sector sees. Private sector, government and law enforcement together create a powerful combination in the fight against transnational organized crime that is often fueled by the robustness of distributed computing and the messaging infrastructure itself.

The spirit of private sector trusted cooperation with government and law enforcement also comprises the FBI's InfraGard program, with the successes and challenges of past and present, as well as the efforts made with the Department of Homeland Security to engage the InfraGard membership in the creation and implementation of the National Infrastructure Protection Plan. This talk will also explore some "real world" examples of technology from the private sector that highlights private sector employees working closely with government to identify and address transnational organized crime that can affect several infrastructures.

Protection of critical infrastructure requires a combination of policy and technology driven by the researchers, owners and operators: everyone has a role in protecting our way of life.

—