

To Help Battle Terrorism, Public and Private Sectors Expand Information Sharing Efforts

September 13 2002

By Dave Pelland, Managing Editor, Electronics Insider

Initiatives launched after the Sept. 11 terrorist attacks to help the public and private sectors share information about potential security threats to the nation's physical and electronic infrastructure have gotten mixed reviews.

While more government officials and business executives cite the benefits of cooperation, some observers say a number of challenges, such as fear of public disclosure and cultural differences, must be addressed before information flows freely between both camps.

"There's a lot of information being shared about potential threats, particularly threats from [computer] viruses or other things that could assist people conducting information attacks," says William Crowell, a former deputy director of the National Security Agency and now president and CEO of Cylink Corporation, which provides information security products.

"The whole sharing mechanism has been beefed up," he says.

Because businesses and government entities have become so dependent on information technology, the differences have blurred between protecting information systems and physical infrastructure. For instance, concerns have been raised that a coordinated cyber-attack could cripple communications systems and hamper the response to a violent terrorist incident.

"Since 9/11, everyone understands the danger of a physical attack, and a lot more people are starting to focus on how an information attack could exacerbate that situation," Crowell says. "This has received a lot more attention in the government and the business community."

Crowell says one promising avenue is the federal Commission on Critical Infrastructure Protection, which was created in 1996 to promote public and private sector cooperation in assessing and mitigating risks to industries such as telecommunications, electric utilities, and banking.

The commission's authority was expanded by an October 2001 Presidential executive order that created the Critical Infrastructure Protection Board, which works with companies in several industries to identify recommended practices for securing vital services.

Crowell also says the CERT Coordination Center, operated by Carnegie Mellon University on behalf of the Defense Department, has increased its threat-related briefings on Internet security issues to the private sector. Another public safety organization that has been active in the past year is InfraGard, which promotes information sharing between local FBI field offices and businesses.

SEARCH

ADVANCED

GO ►

MORE...

Permission-Based E-Mail Marketing Back From Brief Pause

JULY 6 After a brief hiatus following anti-spam legislation, permission-based e-mail marketing campaigns are rebounding.

Audit Committees, Candidates Ease Into S-O Expert Rules

JUNE 29 The audit committee financial expert position has taken on increased importance in the wake of new regulations and greater corporate governance.

Governments Transforming Online Operations

JUNE 21 Government entities are revamping their Web sites to integrate operations and to complete transactions and information requests online.

Regulatory Tech Costs Cause Big Problems for Small Banks

JUNE 16 America's community banks are finding it too expensive to keep pace technologically with myriad new regulations being issued out of Washington.

With Silicon Replacements Years Away, Electronics Companies Continue Nanotech Research

JUNE 4 Nanotechnology will probably have its most immediate effect on miniaturization and performance, not semiconductors.

Health Plans Give New Technology an Earlier Look

MAY 27 Health plans are evaluating medical technology that is still in development, hoping to avoid future surprises.

Security Firms Fighting Network Spyware

MAY 20 Spyware has become the latest problem to plague corporate networks.

But a number of obstacles are hindering efforts to create a unified structure for exchanging information. One of the major hurdles is uncertainty among businesses about how the government would handle information they pass along, according to John Cohen, president and chief executive of PSComm LLC, which does security consulting with state and local governments, and who is director of the Progressive Policy Institute's Community Crime Fighting Project.

"A number of corporate security people are hesitant to share information with the government because they're concerned that if a threat becomes public, that could impact the value of the company's stock," Cohen says. "Businesses want to be sure that their information is handled in a way that doesn't affect them from a business perspective."

To help alleviate concerns about public exposure of data, U.S. Sens. Robert Bennett (R-Utah) and Jon Kyl (R-Ariz.) have sponsored legislation that would exempt information shared with the government from becoming disclosed publicly under the Freedom of Information Act. Critics of the bill, including the Department of Justice and the Electronic Privacy Information Center, say companies could use the bill's information-sharing protections to hide documents from federal regulators.

In addition, getting businesses to share information can be difficult. Cohen says companies that are fierce competitors can be hesitant to share information about potential vulnerabilities.

"If I work at Bank A, am I going to be willing to tell someone at Bank B that the integrity of my information system could be a risk?" Cohen says. "It's very difficult to have competing companies come together, even when doing so would be better for them both."

Another potential obstacle is a cultural gap caused by the different roles of the public and private sectors. For instance, Crowell says that government officials tend to have a lower risk tolerance than business executives. While public officials would prefer to create tight security systems, executives are willing to tolerate a certain degree of risk if it helps them achieve business goals.

"They're like fighter pilots who say 'If I'm fast enough, I can just outrun the risk,'" Crowell says of corporate leaders.

And the fact that information security and terrorism-related threats tend to be complex and ambiguous makes them difficult to recognize, according to Steven B. Davis, CEO of consulting firm IT Global Secure Inc. and former network security manager for the U.S. Treasury.

"Business executives are more likely to spend time dealing with concrete business issues than trying to identify and communicate a nebulous threat," Davis says. "The [federal] government is trying to find a technical solution to what's really a policy problem. There's not a good system for sharing information with state and local entities, let alone the private sector."

But information-sharing initiatives can be effective in promoting informal communication in introducing members of the public and private sectors to one other, according to James R. Doyle, president of security training firm Internet Crimes Inc., and former head of the New York Police Department's Computer Investigation & Technology Unit.

"A lot of information sharing comes down to personal relationships,"

Doyle says. "If they work together, more companies have found that they can trust law enforcement with sensitive information, and law enforcement is better aware of their concerns with sharing information. Once you've built that trust, cooperation follows."

PLEASE RATE THIS ANALYSIS

Quality of Analysis

1 2 3 4 5
POOR EXCELLENT

Comments or Questions

Email Address (optional to enable Insiders to reply)

SUBMIT ►

© 2004 KPMG LLP, the U.S. member firm of KPMG International, a Swiss cooperative.
All rights reserved.

[KPMG Online Privacy Statement and Disclaimer](#)