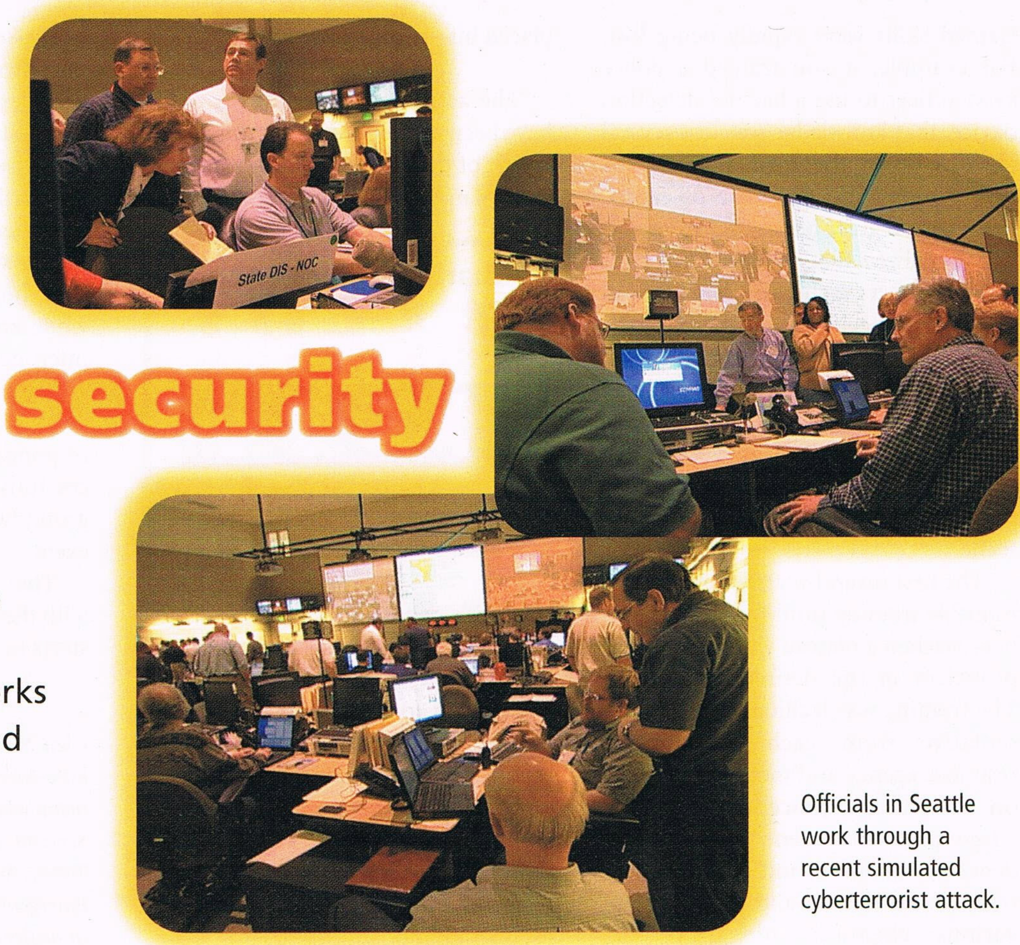
Seeking cyber security



Officials in Seattle work through a recent simulated cyberterrorist attack.

Emergency response agencies continue to make progress in securing their networks against intrusions and potential failures.

By Philip Burgert, Associate Editor

The scenarios have been startling as they have played out in drills, forecasts and the media over the past decade: Terrorists using techniques developed by computer hackers find ways to multiply the impact of their attacks by penetrating and shutting down the computer networks on which public safety and emergency response agencies increasingly rely.

So far though, the scenarios have not materialized. In the eight years since the first magazine mention of a potential "electronic Pearl Harbor" appeared in Time in 1995, there have been no reports of cyber attacks that damaged U.S. infrastructure or seriously affected domestic security operations, the technology program of the Washington-based Center for Strategic and International Studies recently concluded.

While computer security incidents and the economic effects of cyber attacks have been abundant, with 217,394 such events tallied by Carnegie Mellon University's Computer Emergency Response Team between 1996 and the first quarter of this year, none of the incidents has resulted in the public acts of violence, widespread shock or horror in the minds of victims that are required for them to be regarded as terrorist actions, according to James Lewis, senior fellow and director of the CSIS technology program.

Still, this doesn't mean it's time to for law enforcement, fire and EMS agencies to let down their guard in protecting their computer assets and network infrastructures from viruses, denial-of-service attacks and other security breaches that can disrupt and degrade services at times when they're critically needed.

Increased awareness

"There is an increased awareness of the hacker and the cyberterrorist," says Edward (Ed) J. Appel Sr., vice president and COO of the Joint Council on Information Age Crime, San Jose, Calif. <www.jciac.org> He notes that the differences between common hackers and cyberterrorists include the potential for the latter to have considerably more resources and the backing of nation-states.

"We haven't seen cyber attacks that are widely recognized as cyberterrorism," he says. "People are not so sure it's that great of a threat because it hasn't happened yet." But at the same time most agencies are now conscious, he says, of the need to toughen systems to make it less likely that a computer security issue will cause problems, whether it involves a teenager down the block or a technical failure.

Appel authored a guide for responding to cyberterrorism and other computer events that was issued by the council, a non-profit organization with board members representing the International Association of Chiefs of Police, the Justice Department's National Institute of Justice, the security industry and academia. <www.jciac.org/docs/theguide.pdf>

The biggest problem law enforcement agencies have is keeping systems running around the clock, Appel says, noting that maintenance of most computer systems is done late at night, but for law enforcement that can be among the most critical times of day. "They've got as much of a problem from bugs and quirkiness in the software as they do from potential cyberattacks," he says.

Improvements needed

Harlin R. McEwen, a retired police chief who is chairman of the IACP's communications and technology committee, acknowledges that the state of computer and network security varies between agencies around the country, depending in part on financial resources and the ability of the agencies to upgrade to current technology standards. "The police network in this country is not high as far as security is concerned," he says. "Much more strict security requirements still have to be met on the local and state levels."

Also acknowledging that computer infrastructure protection has declined as a priority is Tom Olshanski, a spokesman for the U.S. Fire Administration's Critical Infrastructure Protection Center, in Emmitsburg, Md., which emphasized cybersecurity when it was created under a presidential directive three years ago. "Our focus has shifted to physical security at the Information Analysis and Infrastructure Protection Directorate of DHS, and DHS has tasked its Chief Information Officer's office with the primary role in cyber security." Since then, he says, physical security of personnel and assets has come to be seen as a more focused responsibility of the CIPC.

"Seventy-five percent of the personnel in our fire departments are volunteers, and many are not using computers every day in the fire house," he says. "Volunteer firefighters are not as worried about computer assets, but many career departments and ambulance companies are more concerned. Our job is to meet the needs of both." The CIPC issues information to fire and EMS agencies on updating and improving computer systems security, but has heard of no such security problems in about the past two years.

Appel recounts that the first emergency response plan for computer infrastructure protection was written with the FBI's assistance two years ago. "One of the first things encountered fairly quickly was the realization that some departments lack the ability to assess their state of security," says Appel, who notes that 80% of law enforcement agencies have 25 or fewer sworn officers and that many of them are dependent on other entities such as state agencies, counties or local governments for information systems.

"Some even lack information systems," he says. "We were concerned that IT people are not attuned to or sensitive to the needs of law enforcement and that these systems might be more prone to being attacked."

Awareness raised

Since then the council, the IACP and the National White Collar Crime Center in Richmond, Va., have been conducting an awareness program at the federal, state and local levels. One part of that was a workshop at the IACP's convention late last year that provided police chiefs with a checklist of questions to ask about departmental data, determining when data is compromised, detecting and preventing attacks and controlling access to department systems. Among the security systems recommended were firewalls, intrusion detection, logging, access controls, encryption and personnel reviews of staff with access.

"While everybody is trying to button down their systems, everyone has the same problem," Appel says. "It is hard to design security when the sys-

Exercise tests interagency cooperation

A simulated cyber attack on Seattle-area government systems ahead of May's national TOPOFF 2 mock terrorism event produced what an organizer described as "excellent results in terms of coordinating response to cyber events."

Representatives from the Seattle Police Department, King County Sheriff's Office, state and county emergency management offices, the FBI, the Department of Homeland Security and Canada's Office of Critical Infrastructure Protection joined information technology, transportation and utility officials, as well as representatives from such private-sector companies as Microsoft, Boeing and Qwest Communications in staging the two-day test.

"What we did in Seattle was work through the incident response organization that the stakeholders there feel they need to handle cyber events," says Andy Cutts, technical program coordinator for exercise and scenario development for the Institute of Security Technology Studies at Dartmouth College, Hanover, N.H., which planned the drill. "What we were trying to do was set up a scenario calling on people to work together and make the right decisions under stressful conditions."

The test gathered 150 top decision-makers at a National Guard camp near Seattle to experience a real-time simulation of widespread, escalating cyber events including varying levels of computer load, distributed denial-of-service attacks, virus attacks, breaching of security, cutting of network connections, defacing of Web sites and hijacking of services over the Internet.

Participants found they could best mitigate the effect of attacks when they worked across local, state and federal agency levels, Cutts says. "My view is that responding to these kinds of attacks is more of an interorganizational process than it is a use of technology. To get them to have a more coordinated response is the key."

The agencies are still gathering data from the drills, with complete results expected to be reported in several months, a spokeswoman for Washington state's information services department says.

"Seattle has very high awareness of cybersecurity," says Ed Appel of the Joint Council on Information Age Crime. Microsoft has recently been training employees as well as law enforcement and emergency workers in the area to have a much higher awareness of security, he says, noting that the leading software company has recently "undergone a sea change" in its approach to security that has made computer security a strategic target for the company.

"They deserve some credit," Appel says, noting that the company has spent an estimated $200 million on retooling for computer security. "It's time to call attention to the fact that they are trying to solve the problem now for law enforcement and other computer users."

tems didn't start secured. They were designed to push and pull information, not for security."

Increasingly, the trend is also toward linking computer systems between agencies to aid in coordination of emergency response. While interoperability of first responder radio-frequency communications systems has received considerable attention in recent years, less focus has been applied to communications between agencies involving computers and the security risks those links create.

Appel notes that computer systems for telecommunications are an essential part of the public safety and emergency response agency infrastructure and that while concerns about 911 systems security have received considerable attention, their ties to multiple agencies have in general kept them well secured. Despite the destruction of the emergency operations center in New York City on Sept. 11, the city's 911 system continued to function normally. Appel notes this was because it had been hardened and made redundant, given back-up functionality and made capable of handling 5,000 calls per hour by iXP Corp., Princeton, N.J.

Multi-agency nets

The main efforts in creating multi-agency computer networks have involved what are described as rolling databases, which provide multi-agency responses to queries from squad cars and other emergency vehicles. But, as usual, Appel says, the general complaint within law enforcement and emergency response agencies is about lack of money and lack of control over these systems.

> **"The thing that protects these systems isn't so much that people have done enough with their computers and networks, but that they have good back-up plans."**
> **— James Lewis, Center for Strategic and International Studies**

The resiliency of multi-agency 911 systems was shown earlier this year when computers used by Seattle's emergency dispatch system were slowed but not brought down by the worldwide effect of the Slammer worm. The computers that were hit were used by dispatchers to log calls but response time by emergency services was not affected and the dispatchers quickly switched to use of paper logs, as they would in a power failure.

"Overall the thing that protects these systems isn't so much that people have done enough with their computers and networks but that they have good back-up plans that depend on phone and radio networks rather than computers," says the CSIS's Lewis. "The thing that managers need to do every time they upgrade their computer systems is ask if they've become more dependent on the computers and what would they do if the systems failed."

One extensive example of multi-agency work involving computer network is the example of Capital Wireless Integrated Network (CapWIN), a partnership between the states of Maryland

and Virginia and the District of Columbia to develop an integrated transportation and public safety information wireless network that allows messaging and database sharing to fire, EMS and law enforcement vehicles throughout the region. [*Ed.: For more on CapWIN, see the Sept/Oct 2002 Technology column.*]

> **"While everybody is trying to button down their systems, everyone has the same problem. It is hard to design security when the systems didn't start secured." — Ed Appel, COO, Joint Council on Information Age Crime**

George Ake, program director for the initial two-year CapWIN program based at the University of Maryland in College Park, Md., says the program is very concerned about security and designed to meet or exceed all security requirements specified by the FBI. IBM, integrater of the multi-state network, is also placing top priority on the need for security, providing encryption and secure authentication facilities to prevent unauthorized information access and system intrusions.

Messaging operations and criminal data sharing across an initial network of 22 mobile computers in fire, law enforcement and freeway service vehicles from 10 agencies in five jurisdictions is expected to begin this summer with access to additional transportation and hazardous materials databases added by the end of the year, Ake says.

Local approvals

Winning approvals from local government executives for the necessary middleware, hardware and software to work with multi-agency computer networks is a relatively difficult process that involves convincing local information technology and emergency operations officials to agree to provide updatable and interactive systems that share local data with state and other agencies.

"We are very concerned about keeping the networks up and keeping them accessible while making sure they are closed to outsiders," says Ake, who describes the network as a private wireless intranet. "Security is increasingly a problem we have to work together to accomplish."

JCIAC's Appel notes that community resistance has also sometimes been encountered to proposals for multi-agency sharing of information, with examples being such cities as San Francisco and Denver, where political issues have been raised about sharing of intelligence after bans on such sharing had been enacted several years ago.

"The effort under way now is to improve the wireless mobile data terminal system to provide access to anything that the police would be allowed to see," says Appel. "The vendors want to sell new and better products while the police want to use best practices to improve and secure what they already have." HPP

Philip Burgert is HPP's associate editor and an Oak Park, Ill.–based freelance writer and editor specializing in technology subjects.