

States fight against cyber-terrorism

Cyber-attacks could intensify a terrorism attack and severely damage the nation's ability to fight crime.


BY ED JANAIRO

As the need grows for stronger domestic security, the states must shoulder greater responsibilities to safeguard their residents. With this greater concern for national defense, many state officials are beginning to recognize that cyber-security, the protection of information systems and data from malicious hacking and other types of cyber-attacks, plays a crucial role in the nation's overall welfare.

So far physical attacks against people and communities have posed greater and more immediate threats than attacks against data. Nonetheless in a high-tech world, thousands of information systems, operated by the private and public sectors, ensure the smooth flow of daily life. "Destroy the networks," said former Gov. Tom Ridge, director of the Office of Homeland Security, "and you shut down America as we know it and as we live it and as we experience it every day."

But not only do cyber-attacks act as "weapons of mass disruption," they also can intensify the harm caused by a physical attack.

Former Virginia Gov. James Gilmore, chair of a special congressional commission to examine the country's preparedness against terrorist threats, acknowledged the possibility that cyber-attacks would exacerbate the effects of conventional attacks. "Communications, if disrupted," he said at



States are responsible for protecting communications infrastructure for public health and criminal justice.

press conference in September, "could have significant impact on the [physical] attack itself."

As a result, the Gilmore Commission, officially known as the Advisory Panel to Assess Domestic Response Capabilities on Terrorism Involving Weapons of Mass Destruction, recommended in its final report, released in December, that the federal government establish an independent commission to advise the president on tighter cyber-security measures for the nation.

Many of the communications networks that help safeguard life and property in times of a disaster belong to the states. "State and local IT departments provide much of the public health and safety services communications infrastructure," said Rock Regan, chief information officer for Connecticut and president of the National Association of State Chief Information Officers. "For example, if the state of New York and the city of New York had been unable to communicate with fire and police units during the World Trade Center attack, the confusion and loss of

life could have been far worse."

New York Chief Information Officer William Pelgrin also stressed the importance of state information systems for the nation's protection at a November conference on cyber-security sponsored by NASCIO. Pelgrin said satellite-assisted geographic information systems played a key role in emergency efforts at the World Trade Center disaster. The quick availability of such information lessened the effects of the disaster and helped expedite recovery efforts.

A successful cyber-attack also could severely damage the nation's ability to fight crime. Today, law-enforcement agencies rely on government networks more than ever. Many states operate with an integrated criminal-justice information network that allows the effective sharing of criminal-justice data across jurisdictions. Most remaining states are implementing such a system (see map). Before these kinds of networks were available for law officials, the inability of most law-enforcement agencies to share data with each other hindered crime preven-

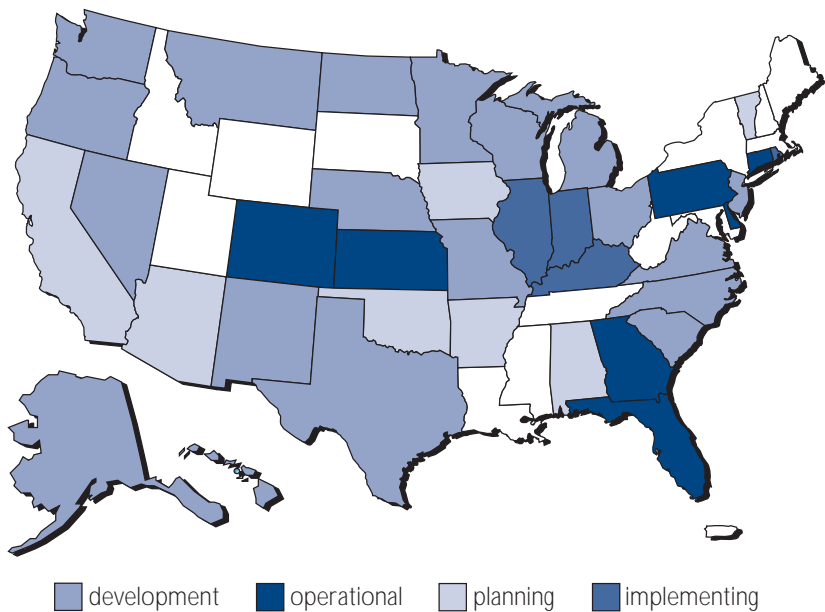
tion. A cyber-attack on criminal-justice information systems could send law enforcement back to the days of miscommunication and missed opportunities.

Further, some cyber-attacks can inflict physical damage. Electric power grids, nuclear power plants and other utilities, for example, rely on secure computer networks. If a cyber-terrorist “cracks” into the systems that control a utility, much harm could result. Recently in Australia, a rejected job applicant at a waste-treatment plant used a laptop computer to hack into the company’s system and caused the release of millions of liters of raw sewage. A local river, park and hotel grounds suffered severe damage. A similar breach of network security at a power plant or airport anywhere could cause much devastation.

U.S. national security relies in large part on the soundness of state government information systems and there has been growing pressure on state IT executives to make these systems secure. During the November NASCIO conference, Regan acknowledged the states’ responsibilities. Referring to President Bush, he remarked, “The president said it very well the other night — ‘The role of government is to protect citizens, and that starts at home.’ States play a significant role in that. We’re the folks on the ground at the local level.”

The men and women charged with much of this responsibility at the state level are state chief information officers, who work with public-safety and emergency-management IT directors. A recently released NASCIO document produced as a result of the November Forum on Security and Critical Infrastructure Protection outlines key recommendations and action items that will help ensure the protection of state networks and ward against cyber-terrorism.

One of the noteworthy items in this report recommends that states pursue legislation that is flexible enough to address all forms of cyber-threats, not just ‘cyber-terrorism.’ States also should consider adopting legislation that will mete out penalties commensurate to the real threat of cyber-attacks. The report supports the passage of a bill before Congress that would exempt cyber-security communications with the federal government from Freedom-of-Information-Act access as a



Source: SEARCH, The National Consortium for Justice Information and Statistics

A state’s Integrated Justice Information System (IJIS) is essential to effective law enforcement. Cyber-attacks against such networks would hamper the fight against crime and terrorism. Many states have an IJIS program in place and others are in varying stages of IJIS implementation.

way to foster greater sharing of security information with states.

The report also calls for greater collaboration between state and federal governments to adopt standards for assessing cyber-threats. These standards would assist in gauging what are, and what are not, acceptable risks for owners of information systems.

Finally, NASCIO seeks to communicate to the public and to policy-makers that cyber-security is not simply an IT function. Security is not only the responsibility of a technical department that oversees computer systems. Rather, cyber-security must be considered from a statewide perspective. Executive-level leadership in states must be keenly aware of the critical nature of cyber-security. Further, all e-government or digital-government initiatives must make protection of public data a priority.

The potential harm of a cyber-attack is real. Is, however, such an attack imminent? Though the recent terrorism attacks lacked a cyber component, the NASCIO report cites intelligence gathered by Carnegie Mellon University’s Computer Emergency Response Team, which warned “over time, all types of cyber-threats are likely to increase in frequency and sophistication with different threats emerging at different times from disparate sources worldwide.”

While reasons abound for states to be concerned about cyber-security, some are concerned that states are not yet fully prepared to defend against cyber-terrorism.

“My guess is that no state is where it would like to be on cyber-security. It will take a lot of resources to achieve that comfort level,” Regan said. But the security will be worth the expense. Aware of the trends in cyber-threats, Regan cautioned that “just because the most recent attacks didn’t have a significant cyber ‘angle,’ [that] doesn’t mean the next wave won’t.” ★

Ed Janairo is a technology analyst with The Council of State Governments.

Resources

Gilmore Commission on Terrorism
www.rand.org/nsrd/terrpanel/

National Association of State Chief Information Officers
www.nascio.org

SEARCH, The National Consortium for Justice Information and Statistics
www.search.org