The National Infrastructure Protection Center (NIPC) was established in February 1998 with the mission of serving "as the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures. These infrastructures, which include telecommunications, energy, banking and finance, water systems, government operations, and emergency services, are the foundation upon which our industrialized society is based." The Web site <http://www.nipc.gov/about/about.htm> is packed with useful information for network managers, whether involved in critical infrastructure or not.

NIPC supports information sharing among government, law enforcement, academia and business. It supports the InfraGard program that has been growing throughout the United States with the help of local FBI offices; as the Secretary of the Vermont InfraGard, I have been delighted to see the growth in participation in our meetings since the initial discussions a year ago. See <http://www.infragard.net/> for more information about that program.

NIPC provides three levels of warnings about threats to the infrastructure: Assessments (awareness materials), Advisories (recommendations for security improvements) and Alerts (news about specific attacks in progress or anticipated soon). These documents may be received by e-mail subscription at no cost and are available on the Web <http://www.nipc.gov/warnings/warnings.htm>.

In addition, NIPC offers free security publications <http://www.nipc.gov/publications/publications.htm>, mostly in Acrobat PDF, including the CyberNotes <http://www.nipc.gov/cybernotes/cybernotes.htm>, which are published every two weeks and which provide an excellent summary of top-priority issues in our field. Archives of all the issues are available online.

On the page marked "Legal Issues" <http://www.nipc.gov/legal/legal.htm>, NIPC provides summaries of important computer crime laws, guidelines on searching and seizing computers, and some pointers to resources on information security education and training, including "Safety Tips for Kids on the Internet."

The Major Investigations page <http://www.nipc.gov/investigations/investigations.htm> gives details of the most current arrest and prosecution of computer criminals. At this writing, there is a fascinating account from the 14th of August 2001 of the arrest of two Khazak nationals arrested in London and charged with breaking into the "Bloomberg computer system in Manhattan in an attempt to extort money from Bloomberg."

NIPC Incident Reports <http://www.nipc.gov/incident/incident.htm> are a method for systematically describing a computer security incident and submitting your report to the NIPC and the FBI. In addition to serving a useful function in keeping law enforcement up to date on the current situation, these reports can serve internally as a model for all incident reporting,
whether transmitted to external agencies or not. I must emphasize, however, that the value of contributing to the common stock of knowledge about computer security breaches is greater than ever due to the apprehended threat of cyberattack on resources of the United States and other countries in the wake of military action against terrorists worldwide. Please do your part as good corporate citizens to keep America strong by reporting computer crimes promptly.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@compuserve.com>. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at <http://www.mekabay.com/index.htm> for papers and course materials on information technology, security and management.

Copyright © 2001 M. E. Kabay. All rights reserved.

Permission is hereby granted to *Network World* to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.