With the nation being called upon to participate in Homeland defense, network managers can play a role by protecting corporate resources against sabotage and disruption. In today's column, I want to summarize what I see as the top priorities for maintaining or improving security in the network operations center.

Starting with physical protection, examine the ease of access to the building where your network equipment is centralized. If it is possible to keep cars and trucks from stopping directly in front of your main entrance, you can install some sturdy concrete obstructions to give your building a few extra yards of protection against an explosion. For example, a few concrete cylinders anchored to the pavement with steel rods could make your building a less attractive target for a car-bomb driver. At the least, the extra distance could reduce the severity of damage from an explosion. You can even put potted plants on top of the concrete to reduce their stark appearance.

On the other side of your building, be sure that your loading docks are well supervised and that all shipments are checked by guards to be sure that they are expected.

As for infrastructure, make sure that external air vents for the environmental control systems are covered with grillwork to reduce the chances of air-borne contamination. Verify that your telecommunications point-of-presence junctions are locked and, if possible, armored against intrusion and damage. Check your emergency power supplies to be sure that they work and that your staff know how to configure the building's power distribution panels to use emergency power efficiently.

If your data or network center has windows on an external wall, now is the time to get those vulnerabilities bricked up.

For large buildings with many employees, press for application of policies requiring all authorized personnel to wear ID badges at all times in the building and to remind employees to report any unknown person who is not wearing a badge.

Remind your staff of the importance of being discreet in all public discussions of corporate affairs, including non-secure mobile phones calls. Be particularly circumspect whenever an unknown person begins asking questions about operations and security. At the office, technical support staff should be reminded never to reveal or reset passwords for anyone over the phone.

Be particularly vigilant about physical access to the network operations center; reduce or eliminate guided tours of your critical work areas. Check your surveillance monitors to be sure that all equipment is working properly. Do not permit cleaning staff, especially contractors whose personnel may change frequently, to have unsupervised access to secure areas.
On the network software side, the single most important protective mechanism you have is to ensure that all appropriate patches have been installed. Use the ICAT Metabase <http://icat.nist.gov/icat.cfm> to check for the right combination of patches for your configuration.

Instruct network staff to be particularly alert to all unusual events reported by your firewalls and by intrusion detection systems. If there is any doubt about the significance of an alert, it should be followed up.

If any of your employees, especially upper managers, have sensitive data on their laptop computers, do your best to convince them to use disk encryption software that will transparently protect those data.

Finally, everyone should be really in evaluating the suitability of their emergency response plants. Make or renew working contacts with local law enforcement authorities; ask your fire department to schedule a site review; update your business resumption plans to include disruptions from bomb Hoaxes or threats of biological contamination. To the extent possible, run tests of your disaster recovery plans.

* * *

Even if you disagree with the particular suggestions in this article, my list will serve a good purpose if it makes you devise and implement your own set of priorities for protecting America's infrastructure.

Whether we like it or not, every one of us is personally responsible for protecting our country.

* * *

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.