In this series, we are looking at how physical security can support the security needs of network operations centers (NOCs) and data centers (DCs). Today's brief note is a continuation of a sub-series on electrical power and related topics.

Common sense (as well as workplace safety regulations) dictates that you install adequate emergency lighting for all work areas and escape routes. After the bombs exploded in the World Trade Center in New York in February 1993, thousands of people had to feel their way through smoke-filled, pitch-black stairwells. It seems the emergency lighting system was controlled by computers that had been blown up by the explosion in the parking garage. Independent lights with their own batteries would have saved time and reduced injury in that disaster. Portable flashlights supplied to emergency marshals would have helped, too.

Now that you've spent all this money on electrical power equipment, how about protecting it all from tampering? Keep all electrical junction boxes, breaker panels and main switches under lock and key. In one hospital information security evaluation a decade ago, I recall bringing the head of the intensive care unit into the hallway and pointing at a panel on the wall. "What's that?" I asked. She shrugged and said, "I dunno; an electrical panel, I guess." "Open it," I said. She did (it was unlocked). When she saw the labels on the breakers her pupils dilated and she looked horrified: those breakers controlled the precious equipment in her ICU B respirators, controlled-injection pumps for intravenous drips, heart monitors, external heart pacematers B the works . If someone had tripped those unguarded, unprotected breakers, some of her patients would have died instantly. Moral: if you care about your electrical power, you have to protect junction panels just as strongly as any other component in the circuit.

If you have to install additional power cables, ensure that they're pulled through protective ducts or manifolds, not left lying about in the suspended ceilings where anyone can get at them. And document all the switches and breakers correctly and readability so that people can make intelligent decisions in an emergency.

Label your UPS and power conditioners plainly with warning signs to prevent unauthorized equipment from being added to the circuits. In the May 1993 session of one of my Information Systems Security courses, a participant reported that an operator plugged a vacuum cleaner into the nearest electrical outlet, overloaded the UPS, and took down the LAN for a few minutes. That nearest outlet happened to be in the server's UPS, but the staff member had no idea that there was anything special about that outlet. You can't blame people for errors when you've failed to provide both training and proper labeling.

Next time, some miscellaneous notes on emergencies involving electricity.
Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Copyright © 2000 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.