This is one of a series of short notes on physical security for network managers. Physical security looks at aspects of the environment in which we work and where we place network components. In this segment, we consider the problem of labeling of critical network and system components.

* * *

One of the perpetual debates in INFOSEC is the value (or worthlessness) of what practitioners call "security through obscurity." The question is whether one can improve security by hiding information. For example, does it help to hide the details of an encryption product so that no one can easily find the algorithm? Dr Dorothy Denning enunciated what many of us call Denning's Law: that the strength of a cryptographic algorithm must not depend on its secrecy. A corollary of Denning's Law is that the validity of an implementation of a strong cryptographic algorithm can best be evaluated when the details of that implementation are accessible. In other words, distrust proprietary implementations of cryptography -- there may be mistakes concealed in the object code that would leap out at (and be fixed) if the source code were made available for inspection.

Well, it's a long way from cryptography to building layout and physical security, but there is a connection. Some aspects of the layout may fruitfully be concealed to make the job of the attacker harder; however, some of the information about buildings ought to be available to improve emergency response.

Specifically, once you've built the computer room, be sure the local fire department knows exactly where it is. Keep your plans, including layout, up to date and coordinate with the fire marshals in your municipality.

However, there is no reason to mark the computer room with special neon flashers that read, "THIS WAY TO MILLIONS OF DOLLARS OF VULNERABLE EQUIPMENT." When I led a delegation of Japanese data center managers to visit the headquarters of EDS Inc. in Dallas in 1991, I was much struck by the anonymity of the equipment rooms. We walked through immense corridors with identical, boring metal doors, each marked with a numbering scheme. They all looked as if they could be broom closets. Then we'd open one up and find vast gleaming, sterile chambers of white tiles with and filled with huge CPUs -- silent titans standing in rows with blinking red and green eyes. Today, I suppose, the same processing power would fit into someone's desk and look like a boring little box with a few holes and slots scattered around the surface.

The theory was that anyone who needed to know where the computers were knew where they were; why help anyone else locate such an inviting target?

* * *

Michel ("Mich") Kabay, PhD, CISSP can be reached by e-mail at <mkabay@atomictangerine.com>.

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.