Physical Security:
Windows

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

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 about windows.

* * *

Don't put windows in your network and data centers. I've already pointed out that there should be no outer walls in your computer room, let alone windows. Windows are physically weak; their frames are weak; and they let too many people see how you've laid our your equipment -- including your security equipment.

I recall one manufacturing site where I stopped next to the floor-to-ceiling windows around the computer console room and stared at the five meter banner on the wall. It had huge numbers printed on it. I asked, "That's not the main modem number, is it?" Yup. So much for dial-in security.

Unfortunately, many executives who worked with computers in the 1960s and 1970s or who base their standards on Hollywood movies still think that vision panels make their data center look more impressive. If you are faced with this retrograde attitude, try a graduated approach to getting rid of these vulnerable spots in your defenses. Offer the decision makers a choice between, say, concrete, brick or bullet-proof safety glass. Alternatively, you can strap the executives down and force them to watch endless loops of Bruce Willis surviving the destruction of the Glass House in the movie "Die Hard."

If you cannot get approval to remove the windows in your computer room, install vertical blinds and keep them closed all the time except when there are important official visitors pressing their noses to the glass. Install security glazing (shatterproof metal-reinforced glass), and perhaps gratings securely attached to the walls. Install breakage sensors and connect them to the main building alarm systems. Aim motion sensors and closed-circuit television cameras at the windows. Move equipment whose presence should be secret away from the windows. Install a few dummy security cameras and motion sensors just to keep spies and intruders guessing.

There are a couple of other reasons why high-security sites do not permit windows in their NOCs and DCs. An obvious point is that external windows offer opportunities for snipers to attack individuals. More subtly, windows vibrate as people talk; using laser interferometers, it is possible to measure those vibrations and reconstitute the sound waves that caused the vibrations. Thus an exterior window provides an easy way for industrial or other spies to eavesdrop on conversations from an observation post far away in another building. However, don't try to persuade your top officials to give up their corner offices -- some advice is just too unpleasant to bother presenting to upper management when the risks are low. I think that such advice might get you sent to the staff psychiatrist in most organizations.

What might work is to suggest that a window-rich office is perhaps not the best place to discuss top-secret strategic plans with catastrophic consequences of unexpected disclosure. People talking about make-or-break information would do well to do so in sealed rooms with no windows. The key is to be reasonable and not to apply security rules unthinkingly.

* * *

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.