Physical Security:
Walls and Doors

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 walls and doors.

Walls

When you build an enclosure for expensive and critical equipment, be sure they're substantial walls, not mere drywall partitions. Reinforced concrete that runs from slab to slab is best. Be sure the design allows for no crawl spaces around the wall above a drop ceiling or below a raised floor.

Check your plans and forbid any closets in the walls of your NOC or DC; they are weak spots and also provide concealment should anyone decide to punch through the wall using drills or explosives.

Finally, if your security needs are usually high (or if you have been watching too many action movies), talk to your architect about the design of the outermost walls of your building. Avoid chases (decorative indentations on the side) and other features such as rusticated stone that could make it easier for assailants to use mountain-climbing techniques to climb your building.

Doors

Have as few doors as possible. You must know and obey all the safety regulations which mandate the number of exits you must include for protection of human life. Your architect will know what the law requires. However, only one door should be used for entry and normal exit. All the others should be used as emergency exits only. All doors should be equipped with crash bars and alarms and decorated accordingly. You can even buy signs that read, ADOOR IS ALARMED,® (which always make me want to pat the door and reassure it that everything will be OK).

Choose heat-resistant doors (solid metal or thick metal with a structurally-sound core) and avoid any glass if at all possible. If safety regulations require glass panels to prevent smashed noses, insist on multiply-laminated bullet-proof, shatterproof small panels. Glass is a weak point anywhere in the secured area.

Installing a door that would make your local bank proud will be pointless if the frame is so weak that it -- and the door -- can be pried out of the wall with a crowbar. Door frames should be anchored solidly in the wall; if possible, bonded to the structural members of the wall. Door hinges should be on the inside of the secure area so they can't be dismantled. Choose hinge pins that are welded into place -- not the ones that can be unscrewed and removed by anyone with a home tool kit.

Protect door locks with astragals (a lovely word meaning the edge-plates that prevent nasty folk from inserting credit cards, screwdrivers and chisels into the latch and forcing the door open). I have seen many sites which use astragals which extend from top to bottom of the door to provide maximum protection.

Don't use motion or simple proximity sensors to unlock or open doors into secure areas. Sliding doors controlled by such sensors -- like those used in many public buildings -- can generally be opened from the outside simply by pushing a sheet of paper through the rubber gaskets and waving it about.

* * *

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>.