Physical Security: Layout

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 how to position equipment and services within the center.

* * *

Within your data center, try to put separate functions in different compartments. For example, keep printers away from consoles, disk drives, processors, patch panels and server racks: the paper is a fire hazard and the paper dust gets into your air filters.

To ensure that you don't wipe our your backups if there is a disaster in your NOC or DC, put tape vaults and data safes far away from your disk drives. However, you can reasonably have a local fire-proof safe or vault for the convenience of operators as long as the tapes stored there are not your latest backups.

Put your access-control equipment into a separate, high-security area, not with the rest of the computers. Security measures should reflect the potential exposure (consequences) of compromise; since access to the security equipment compromises everything else, it makes sense to guard it even more strongly than other components of your networks and systems.

Position your phone switches away from the computer room so that a single attack cannot put your entire operation into jeopardy. This suggestion follows the principle of reducing the number of single points of failure -- more humbly known as not putting all our eggs in one basket.

The lower the traffic through a secure perimeter, the lower the risk of failure. Accordingly, try to keep your operations personnel comfortable inside the secure areas surrounding your equipment as much as possible; for example, include rest rooms, eating areas and office space for the staff who run your production systems within a tightly-controlled space inside the perimeter. This recommendation does not mean that you should forbid staff from leaving the secured area on their off time -- that's their perfect right. However, the availability of such facilities will be convenient for some of the staff some of the time and will contribute to lowering the risk of intrusion and increase the speed of response to emergencies in the NOC or DC.

* * *

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.