Physical Security Nightmares

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

It's always a pleasure to receive thoughtful and stimulating e-mail from readers of this newsletters. Recently, I received a heartfelt appeal from a physical security expert to network and other computer system administrators. Jeff Anderson, President of ACI International Inc. (<http://www.aciconnect.com>) wrote the following essay that I believe will interest readers. Mr Anderson's company specializes in PC-based video surveillance systems.

* * *

As I read your newsletters, I feel that the subject of physical security is not being addressed adequately, especially in light of 9-11. I have spent decades serving the security needs of our clients around the world, and I can tell you point blank that the tightest firewall, intrusion detection system, or password protection scheme is useless if an intruder (or employee) can gain physical access to vital systems unchallenged. Let me give you an example or two.

I recently visited an office of a large multinational organization where I was asked to review their physical security. On arrival, I merely mentioned the name of the person I was coming to visit and signed a guest registry. I was not asked for identification documents. At that point I was given access to a conference room where I was asked to wait alone for the individual with whom I was to meet. Across the open-plan office I could see a large computer room. I could have easily strolled across the office and entered the computer room even though I was an outsider -- a complete stranger.

On another occasion I was invited onto a high-security facility and was required to produce my security clearances before being permitted entry. In spite of my long held military level security clearance, I was issued an "escorts only" pass, which allowed me entry to the facility, but only as long as someone in authority stayed with me. I spent two days there. On the first day, I was escorted everywhere -- even to the restroom. I was given a desk from which to work and each time I had to leave that desk an escort came along with me. No problem. However, on the second day, the escort rules seemed to have softened considerably; for example, I visited the restroom unescorted. Later that day, I was escorted into a secured computer room where I was asked to look at a particular computer. Shortly after I arrived in the room, my escort was distracted by an urgent cell phone call and left the room. I was left sitting in a computer room surrounded by computers presumably containing sensitive material and there was no one there but me. There were no surveillance cameras in that room. I had 15 minutes to myself in there. After 15 minutes, two gentlemen came in, said hello, and sat down at computers and started typing. I was wearing my "escorted only" pass on my lapel but no one noticed. My "escort" returned five minutes later.

I can't even begin to count the number of times that I have been in a facility with card access control heavily deployed and had someone hand me their access control card so that I could go into the next room and place a call, or visit the restroom, or go grab a coffee.
Another problem I encounter is people in the physical security industry who don't know much about computers. For example, as you may know, we manufacture a PC based security control system. We recently received a call from a security professional who had encountered one of our systems in the field and didn't know how to use it. When the customer asked him how to perform a simple function in software, rather than admitting that he did not know, rather than opening the manuals and reading, rather than consulting the help files, he simply started randomly pressing every key on the keyboard, eventually causing the system to do something unwanted. He called us at that point to tell us that our products don't work. I wish I could call this an isolated incident. I can't.

In summary, it seems to me that

* Physical security is not being addressed adequately in today's world.

* Too many security system installation companies are not computer literate (they are not part of the solution, they are part of the problem).

* * *

My thanks to Mr Anderson for the comments printed above and for his permission to quote him verbatim.

Readers may want to review the series of 20 articles on physical security originally published in this newsletter in the year 2000 and freely available in the archives at <http://www.nwfusion.com/newsletters/sec/>. In addition, my colleague Franklin Platt has prepared two magisterial chapters on physical security for the soon-to-be-published Computer Security Handbook, 4th Edition, edited by Seymour Bosworth and myself. The 1200-page text is due in bookshops in early April; the cover is visible on AMAZON.COM by searching on "Bosworth Kabay" (without the quotation marks).

* * *


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@compuserve.com>. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at <http://www.mekabay.com/index.htm> for papers and course materials on information technology, security and management.

Copyright © 2002 M. E. Kabay and Jeff Anderson. 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.