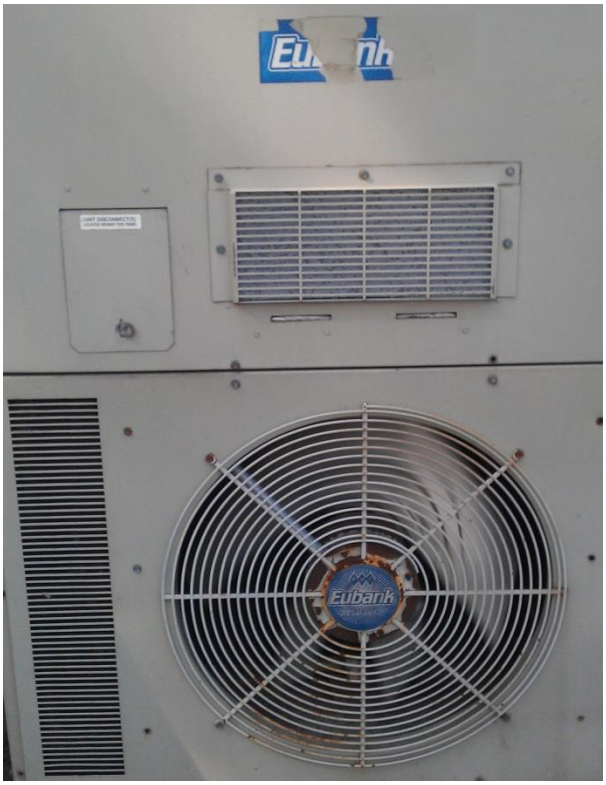
Facilit{ating,ies} Security

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University, Northfield VT

Recently I was at a local shop and noticed a potential problem. See if you can identify it from the picture below showing part of the air conditioner on the outside of the building:



The problem is the unlocked cover to the left of the centre in the photo; it covers the circuit breakers. I asked the shop clerk whether the air conditioning was important for the shop; indeed it is, she said, as it maintains appropriate temperatures for non-refrigerated foods in the shop. The shop has already suffered vandalism; hoodlums broke one of its windows and its glass door during a night-time robbery. Leaving open access to switches that turn off the power for the unit is an invitation for further trouble.

Starting in the 1980s, I specialized in facilities security and in particular, hospital security. The worst case I ever encountered involving an electrical panel was in a Montreal hospital. I called the head of the intensive care unit (ICU) out into the public hallway from her office and pointed at a grey metal panel on the wall. "Do you know what that is?" I asked. She looked at me as if I was crazy. "Yes," she said, "it's an electrical panel," and looked at me as if to add, "Duhhh." I opened the panel and she turned pale: the breaker switches were clearly labelled with the names of critical equipment in the ICU such as heart monitors and iron lungs. If a passer-by had switched any of those breakers off, people could have died. With open access to the public in the hospital, the risk of tragedy was increased by the failure to lock that panel.

Typing < physical security overlooked > into the Google search engine (without the < >) brings up several articles making the point that physical security is often overlooked in today's technology-intensive information assurance. For example,

- Barker, D. (2008). "Is physical security overlooked in lieu of network security?" Tales of a Network Security Engineer – David Barker's blog (5 Sep 2008). < http://areyouvulnerable.com/?p=12 >
- Higgins, K. J. (2006). "The 10 Most Overlooked Aspects of Security." Security Dark Reading (29 Nov 2006). < http://www.darkreading.com/security/news/208808177 >
- Krupa, A. S. (2003). "The Oversight of Physical Security and Contingency
- Planning." SANS Institute Information Security Reading Room. < http://www.sans.org/reading_room/whitepapers/recovery/oversight-physical-security-contingency-planning_557 >
- Posey, B. M. (2003). "Don't overlook physical security on your network." TechRepublic (3 Apr 2003). < http://www.techrepublic.com/article/dont-overlook-physical-security-on-your-network/5032930 >
- Seiden, M. & B. Weis (2004). "Physical Security – the Good, the Bad, and the Ugly." Physical security workshop at 21st Chaos Communication Congress (CCC) by Chaos Computer Club. Berlin, Germany, 28 Dec 2004). Posted to YouTube (2 Jan 2012). < http://www.youtube.com/watch?v=-4IIAKLCN-w > *Meaningful content begins at 03:20 after a load of blather.*

A document I prepared for students and clients is available for anyone to use in security assessments, education or training: "Facilities Security Audit Checklist"< http://www.mekabay.com/infosecmgmt/index.htm >. Major sections include

1. Fire hazards
2. Water
3. Air conditioning
4. Electricity
5. Preparing for civil, man-made, and natural disasters
6. Alternate location
7. Access control
8. Housekeeping
9. Miscellaneous

Checking physical security is relatively easy, but it requires a shift of focus. As in any security assessment, the trick is to notice details that affect assurance; the analyst should be thinking of possible problems and vulnerabilities to malicious insiders and outsiders. The best way to learn is to use a checklist in a walkabout: actually going through a facility looking at everything with a sceptical eye. The checklist may stimulate readers' imagination: just imagine what the Bad Guys could do with that unlocked electrical panel. . . .

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *

Copyright © 2012 M. E. Kabay. All rights reserved.