Physical Threats to the Information Infrastructure (2)

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

In this occasional series, I am showcasing some of the best short essays submitted by students in information assurance and cybercrime courses and programs at Norwich University. John Orlando, PhD, is the Administrative Director of the MSIA (Master of Science in Information Assurance) program at Norwich; in compliance with the policy instituted by Dean Fred Snow, he is participating in the MSIA program as a student. This column is the continuation of a slightly edited version of his report on physical security at Norwich University.

* * *

Man-Made, Malicious, Threats

Intruders have been known to attempt to gain access to a computer system to steal hardware or to vandalize the facilities and equipment. In response, the University’s IT department has adopted a strict policy of not allowing non-IT personnel into the computer center unescorted. To prevent either accidental or malicious harm cleaning people working after hours, all cleaning is done during business hours. Moreover, doors are equipped with alarms and rooms equipped with motion detectors to prevent after hours intrusion. Not even the university’s security personnel have access to the secured areas.

Only the CIO and the IT manager have keys allowing after-hours access to central computing facilities.

The computer labs that are used primarily by students are somewhat more vulnerable to intrusion because lab assistants are not always on hand. Theft would seem the primary motive for intrusion, although someone might also attempt to tamper with a computer in order to gather passwords by using a Trojan horse that simulates the logon dialog. Thus, each lab computer’s CPU is locked to the table that holds it; most desktop computers used by faculty and staff are similarly secured. Most important, the location of the lock also makes it impossible to access the hard drive without opening, or breaking, the lock. This strategy does not absolutely prevent tampering, but it does make it riskier for the intruder and it provides a physical warning that a system may have been modified without authorization.

Recommendations

The IT department at the university has taken many precautions against physical threats to the main computer center, and has placed some protections on the desktop terminals used around the campus. The main vulnerabilities to the University’s infrastructure would appear to lie outside of the computing center. As the IT department is quick to point out, each building on campus has a central box through with all electronic communications are routed. These boxes are normally found in storage rooms or closets. There is no special security around these boxes that would prevent someone from plugging into the lines and intercepting communication. Even worse, a number of people have keys to these rooms, such as maintenance workers and even
regular employees. For instance, many staff members have keys providing them with access to the storage room in Jackman Hall (the main administration building) where the communication box sits. In principle, someone with access to these rooms could install a small device that snoops network traffic and transmits it to a remote location, such as a van packed just off of campus. In light of this danger, the IT department is currently lobbying for funding to install locked screens around these boxes.

* * *

For further reading:


* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.


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@norwich.edu >; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2003 John Orlando. 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.