I’ve been doing facilities security assessments and reports for over two decades and still occasionally get requests for that kind of work. Recently, one of my local clients reported a problem with the two doors on their small Vermont office building. Seems the police in their town found one of the doors unlocked in the middle of the night and called the security firm to get them locked. The manager of this 50-employee medical billing firm sent out a plea to all her employees asking them to _please_ remember to lock the doors when leaving the building. She copied me on her message and here’s what I replied.

* * *

Sally, you are facing the same problems in physical security that information security professionals face all the time: people cannot effectively compensate for a fundamentally flawed technology.

In computing, for example, system managers struggle constantly with passwords. Users create terrible passwords – names of spouses, names of children, names of pets – or use the word “password” itself! No matter how much we try to teach our users about good password hygiene, the problem is that passwords are a _terrible_ way to control access to restricted resources! The whole idea that we should rely on users to develop and execute such an important element of access controls is fundamentally flawed, as any security officer will tell you from bitter experience.

The fundamental problem with the locks on your building is that they are badly designed. The operation to _open the door_ requires _unlocking the lock_. A properly designed lock allows a user to open the door with one method but requires a different method to unlock the lock. For example, the locks on Dewey Hall at Norwich University [where the School of Business and Management offices are located] allow a key user to turn the key counterclockwise to open the door – but that operation leaves the door locked. One must turn the key hard and _clockwise_ to unlock the lock, and there’s a pronounced _click_ that serves as additional feedback to alert the user that the door has been unlocked.

My prediction as a security specialist is that no amount of haranguing will ever solve your door problem; the futility of the lectures is worsened by the complete impossibility of referring to an audit trail that would identify who failed to re-lock the doors: there _is_ no audit trail.

The cheapest solution is to pay for new physical locks with the same keys if possible. Use the same approach as that described for the Dewey Hall locks. However, even that improvement will not resolve the problem: nothing stops someone from accidentally unlocking the door by mistake or from unlocking the door and forgetting to lock it – and there is no audit trail to tell us who did...
it (and thus to help reduce the likelihood that an individual will repeat their mistake).

Given the hundreds of thousands of dollars of valuable computer and audiovisual equipment in the building, coupled with the wealth of confidential information available on paper, on magnetic media and through unsecured network access, I recommend that you invest in two electronic access systems: one for the front door and one for the back door. A proximity-card system would allow authorized personnel to enter the building without difficulty – and would establish an audit trail at the same time without requiring any action by the employees.

The same system would ensure that any employee still carrying the proximity card on the way out of the building (without in any way interfering with the normal exit routine required for safety) would also register a record in the audit trail. The audit trail can be kept on computers controlled by Selim [the techie in the company] using a TCP/IP link to your network. _Egress_ (i.e., outbound) audit trails are useful because they can provide instant information about who is still potentially in the building, thus helping firefighters and police; they also provide information about unusual behavior (Why is Ralph leaving the building at 2 in the morning every day??) that may signal a threat to security (or, for that matter, harm to the well-being of the employee through burnout) and thus help avert problems.

Expect such locks to cost about $2,000 per door (including the computer interface but not counting the cost of installation) and the proximity fobs or cards to cost about $4 each. (See for example http://www.nokey.com/harcon2doorp.html).

I realize that spending this amount of money on new equipment instead of just buying $100 locks is going to be a difficult pill to swallow and a more difficult pill to get authorization for from Frank [the owner of the firm]. However, the damage to your reputation would be serious if local news headlines were to announce that your building had been ransacked because your doors were unlocked. However, given the severity of HIPAA [Health Insurance Portability and Accountability Act] penalties for loss of control over patient data that your employees are handling day after day, you can’t afford that kind of risk.

If patient data walk out the door, so will your clients.

[NOTE: all identifying details of this case have been altered to protect client confidentiality.]

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.graduate.norwich.edu/infoassurance/> and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2008 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.