Final Words from the Field

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

A senior security consultant who prefers not to be identified sent me the following cases in response to the ongoing physical-security series. I think readers will enjoy his stories and his points and I thank him for permission to print them. This is the last of three columns provided by our anonymous benefactor.

* The Underground Data Center *

Initially, the headquarters data center was three levels below ground. When it rained, it often flooded, necessitating a shutdown of the equipment and service to customers. Finally the building was renovated and the center was moved. It was now two levels below ground, under the cafeteria and the two most used restrooms in the building. A break in the public sewer connection just outside the building caused the sewage to backup into the building, closing it for four days and flooding under the raised floor of the computer room. Fortunately, the building closure took place between Friday and Monday, minimizing the impact on 4000 local customers and numerous others with remote access.

Lessons learned:
(1) Don't located critical facilities below ground, under cafeterias, rest rooms or other places where water could originate.

* The Insecure Off-Site Storage Facility *

The off-site storage facility was just off the Interstate, at least 10 miles from the primary site. The neighborhood appeared to be less than desirable. When the review team entered, they noticed a window was broken on the right side. According to the staff, someone had thrown a beer bottle through it the previous evening from the parking lot.

While the team was in the lobby, the front door was opened for local resident, soliciting for some cause. The vault door, approximately 30 feet away from the front door, remained unlocked during the day. Outside, the power shut off was unprotected and the air conditioning equipment in the parking lot had no vehicle barriers or fence. On one side of the building the next lot contained an appliance junkyard, just a few feet from the storage facility. The backup tapes stored there were critical for the successful deployment of its contingency plan at the hot site. The Operations Staff initiated the contract for this facility and the Security Staff had never visited the site.

Lessons learned:

(2) Be sure your off-site storage facility has as strong or stronger security than your primary facility.
(3) Don't sign the contract to use a vendor's facilities until the security staff has visited the site and is comfortable with its security.
(4) Protect power cut-off, air-conditioning, and other important infrastructure support systems.

* The Almost Secure Off-Site Storage Facility *

The off-site storage facility was truly state of the art. The building included only a street number to mark it. The only glass was around the reception area door. Visitors had to be admitted by the receptionist. The vaults had only one entrance/exit, thanks to a security conscious fire marshal. Delivery vehicles entered a large indoor loading dock to unload.

However, a person who wish to illegally enter the facility could use a ruse such as claiming his wife was having a baby in the car just outside the front door and he needed to call for an ambulance. When the receptionist admitted him, he could then threaten her with a knife or firearm, forcing her admits others from the vehicle, and then to use her key card to admit him to the hallway with access to the vaults. Since there are no security personnel on site, it's unlikely that the anything would stop the attackers from entering the vaults and planting a bomb or otherwise damaging the backup media.

Lessons Learned:
(5) Train your receptionist not to be influenced by a ruse at the front door.
(6) If the rules state that the receptionist should admit only visitors with appointments, there are no exceptions; reinforce the training with realistic exercises.
(7) Also, the receptionist's card does not need to be programmed to enter the critical areas. It should grant access only to office areas in the front of the building, not to the operations areas.

Once again, my thanks to the reader who supplied these real-life cases of poor physical security.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.

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>.

author.