Why Data Center Access Control Deserves More Attention

By Elizabeth M. Ferrarini

DATA CENTERS HOSTING CRITICAL SERVERS ARE WHERE THE MONEY IS, and the bad guys know it. But secure access control of the data center often gets downplayed, but it's just as important as the rest of the network infrastructure.

Kevin Beaver, author of The *Practical Guide to HIPAA Privacy and Security Compliance,* says that most people focus on technical security issues with servers in the data center, not realizing that's not the only way to enhance security. He adds that physical security must be included. "You cannot have any sense of information security if you don't implement proper physical security measures," Beaver says.

IT departments may disregard physical security of the data center, deeming it too expensive or assuming that it's someone else's problem. Unfortunately, the confidentiality, integrity, and availability of information can be impaired as a result of unauthorized physical access, damage, or destruction of physical components.

Physically securing the network means limiting access to it. The National Computer Security Center's "Glossary of Computer Security Terms" defines physical security as "the application of physical barriers and control procedures as preventive measures or countermeasures against threats to resources and sensitive information." It should be available only to those individuals who require the network and its components (applications, files, correspondence, etc.) for performance of their stated duties.

Physical security runs the gamut from protection of the power supply via secure conduits to protection of work areas.

Physical security runs the gamut from protection of the power supply via secure conduits to protection of work areas. That protection may be in the form of physical locks, security guards, or any number of state-of-the-art authentication technologies. Systems can be put in place to oversee the entry and exit of employees and visitors via closed circuit cameras or use of monitoring systems. Document shredders (in-house, or through third-party shredding company disposal bins) ensure that sensitive information cannot be examined by unauthorized scrutiny.

KEEP THE DOORS LOCKED TIGHTLY

Effectively controlling physical access to an organization's facilities should be the single top concern for the physical security staff. Most organizations use one or a combination of mechanisms when implementing physical security.

The easiest approach to security may be the most conspicuous. A simple, traditional lock-and-key barrier effectively impedes access to the network. Only those who require access to buildings or particular rooms within buildings are allocated the keys to open their locks. This low-tech approach is attractive not only because it is simple (no specialized training required), but also because it is inexpensive, making it appealing to smaller organizations. Issuing keys that cannot be duplicated adds yet another layer of security. Mantraps, where two doors must be passed through, permitting only one person to pass at a time, add one more security measure to traditional lock-and-key entry.

Unfortunately, low-tech locks and keys come with drawbacks, too. When personnel lose keys (unintentionally by trusted employees, or when keys take off along with former, sometimes disgruntled, employees), the locks will have to be changed and new keys issued. If this happens repeatedly, the costs of issuing replacements may outweigh the benefits of this security approach. Another drawback is that a key can wind up in the possession of someone who does not have authorized access. This may happen either by theft or by an employee who willingly passes it on. If an additional safety precaution is not in place (where the locks are watched over by a security guard or camera, for instance), anyone who holds a key may gain entry.

CARD CONTROL DEALS A MORE SECURE HAND

Electronic key cards and their brethren offer a more technological take to the standard-issue lock-and-key approach to access control. These include smart cards, magnetic badge readers, or just electronically coded plastic cards that are presented to be read by a magnetic card reader. Larger organizations favor key card access because it eliminates many of the management problems inherent in traditional lock-and-key access while also providing a higher security standard.

On the positive side: Key cards are appealing because a single card can control secure access to more than one location, and it's also easy to accommodate large companies that maintain multiple entrances. Some cards do not require your employees to carry a separate key card. This user-friendly and compact reader is easy to program and can control access for up to 1,000 users. An employee's existing credit card, bank card, or driver's license with magnetic stripe can be swiped to gain entry.

In addition, if the organization sees the need, it may opt to keep electronic track of the comings and goings through each of its access points. Another attractive facet of key cards is that if a user's employment is terminated, his card can easily be disabled by the organization, even without return of the card itself.

©2006 Technical Enterprises, Inc. Reproduction of this document without permission is prohibited.

The chief drawback, again, as with everyday locks and keys, is that anyone in possession of a key card may gain access. Although many organizations maintain electronic floodgates, respect for those controls may be lax at best. One IT professional who does not want to be named says that he has seen many engineers pass an access control card between [themselves], bypassing strict rules that require that all personnel who have access to the data center be clearly identified. In addition, maintaining key card systems may be too costly for smaller organizations. Another potential hazard may arise if the central authentication system should fail. In that case, all authorized users will be banned access.

By far the most common drawback of key cards is tailgating, where unauthorized individuals follow closely behind authorized, card-carrying personnel and enter the building right along with them. The dubious added security of a guard overseeing the entrance and electronic reading of cards may be fruitless, as the tailgater may simply flash an invalid card and be waved through without the card being scanned.

HAND PRINTS TELL NO LIES

The biometric approach lends perhaps the most intriguing dimension to the authentication process. Users attempting to gain entry to a facility may be met with a variety of biometric authenticators. A particular physical trait of the user is examined in an authentication inquiry and compared with stored reference data. Identifiers include characteristics of voice, fingerprint, hand geometry, face, and the iris or retina.

Fingerprint readers compare the pattern of fingerprints with those in the database and hand readers examine the shape and size of hands in order to authenticate the identity of users. The biometric advantage lies in the fact that physical traits cannot be altered, copied, or lost, and for the most part are not able to be stolen (except via some gruesome, almost sci-fi-like possibilities). Organizations can find any number of reputable manufacturers in the biometric arena.

AMERICAN WATER RAISES THE PRESSURE ON PHYSICAL SECURITY

For decades, American Water Works Company, the largest operator of water treatment and distribution plants in North American, shuttled school children and customers through its hundreds of facilities in 29 states, Canada, and Puerto Rico. Bruce Larson, American Water's security director, says, "Water was an open business. Each facility has its own security guard, set of locks and alarms."

The events of the September 11, 2001, caused management at the $2 billion company to raise the physical security bar at the 711 treatment plants. Larson says, "We realized that terrorists might kill some of our 18 million customers with our product."

Post 9/11 Bruce Larson undertook American Water's security challenge by becoming responsible and accountable for all physical security, information security, crisis management and business continuity throughout North American operations. He immediately put together a security plan which became the model for the entire North American company, including the treatment facilities. In 2003, American Water became part of RWE Thames Water, the third largest global water resource company.

Here's what Larson, a 17-year security veteran and consultant to a Presidential adviser on Homeland Security issues, had to say about maintaining water tight physical security at the company's facilities.

Q. What does physical security include?

It focuses on the critical operations at all of the water treatment works around the country. Specifically, we look at every aspect of security from access control all the way to control of sensitive documents, and alarms.

Q. How do you know you are getting good access control?

One of our goals includes reducing the need of humans required to provide physical security controls. To this end, we focused heavily on automated access control, automated alarm systems, and automated video systems. To enter buildings, employees go through a turnstile with a smart keycard. Front desk security people spend their time validating the identity of visitors, and making sure they are properly escorted. Since 9/11, we've revised our visitation process at the treatment sites and now focus more on where employees go in a facility.

Q. How do you monitor all of these systems?

We've extensive contracts for monitoring our various systems. All 90,000 alarm points, along with badge access controls and video monitoring, feed into one central computer system. We can access this system anywhere in the business from a Web-based GUI. Our 7 by 24 central command center staff focuses on managing incidents surrounding these alarms. Each facility's monitoring station enables the staff to be the first response source. Because of the diversity of the physical operations sites and the number of false of alarms, we've a standard operating procedure set for responding to alarm signs.

Q. How have you integrated physical security with IT?

We've converged the business processes. However, you're always going to have different sensor systems or control systems, firewalls, and locks on doors. Right now it's passwords and badges. Eventually, employees will be able to use the same access control keycard to log on their desktop PC. Also, if the IT help desk gets a security-related incident, then it's turned over to my staff to manage it.

Q. What does the security staff at a facility consist of?

Every facility has its own set of unique challenges. Some locations might require more physical security guards than other location. Typically, each facility has an operations person who owns the business, including all local security operations, and, as a result, functions, at the central security contact. We also have certified water treatment plant operators who treat the water and make sure it gets distributed. These operators respond to emergency situations first, followed by 911, if needed. An operations person at our command center is also assigned to respond to situation.

Q. Since 9/11, what new things have you learned about emergency situations or security breaches?

Security incidents can cause business crisis and business crisis can disrupt security. For example, if a terrorist breaks into a critical

©2006 Technical Enterprises, Inc. Reproduction of this document without permission is prohibited.

operations facility, then we have a major business crisis. A major hurricane can cause a business crisis and, in turn, affect both physical and infomatic security. Significant amount of operations in the New Orleans areas and have been challenged by that event.

Q. How do you select the security systems you use for physical security?

Whether it's firewall software or a video monitoring system, we use tried and true systems we can configure out of the box. I'm opposed to developing any type of system. Our business is water, not security.

Q. You've just started to get involved in security for some of the parent companies' international sites. How does physical security differ abroad than in North America?

In the U.S., each state has a variety of controls. Likewise, each country has its own set of legislative and regulatory controls for physical security of the infrastructure. Each country also sets a different social responsibility code. Some countries want armed guards patrolling the facility's perimeter. The UK doesn't want to see any weapons.

The financial impact caused by a major crisis can vary substantially. If there's an outage at a water treatment plant in London, then millions of dollars are going down the drain every second. A similar outage might have a lesser financial impact if it happened in Puerto Rico.

NaSPA member Elizabeth M. Ferrarini is an IT consultant from Boston, Massachusetts.

Network Support™
Supporting Servers and Desktop Environments

©2006 Technical Enterprises, Inc. Reproduction of this document without permission is prohibited.