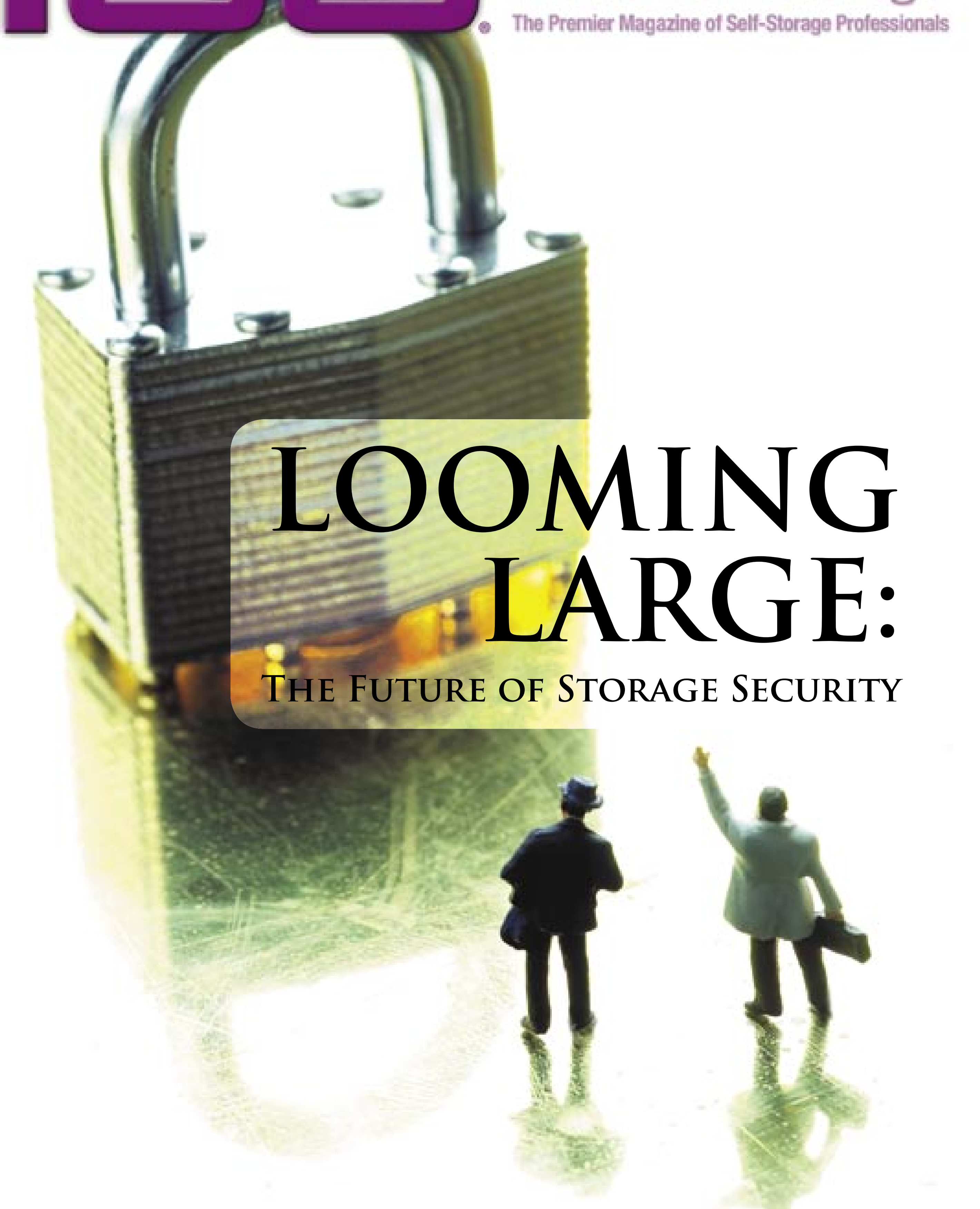
June 2005 www.insideselfstorage.com

VIRGO publishing

ISS®

Inside Self-Storage®

The Premier Magazine of Self-Storage Professionals



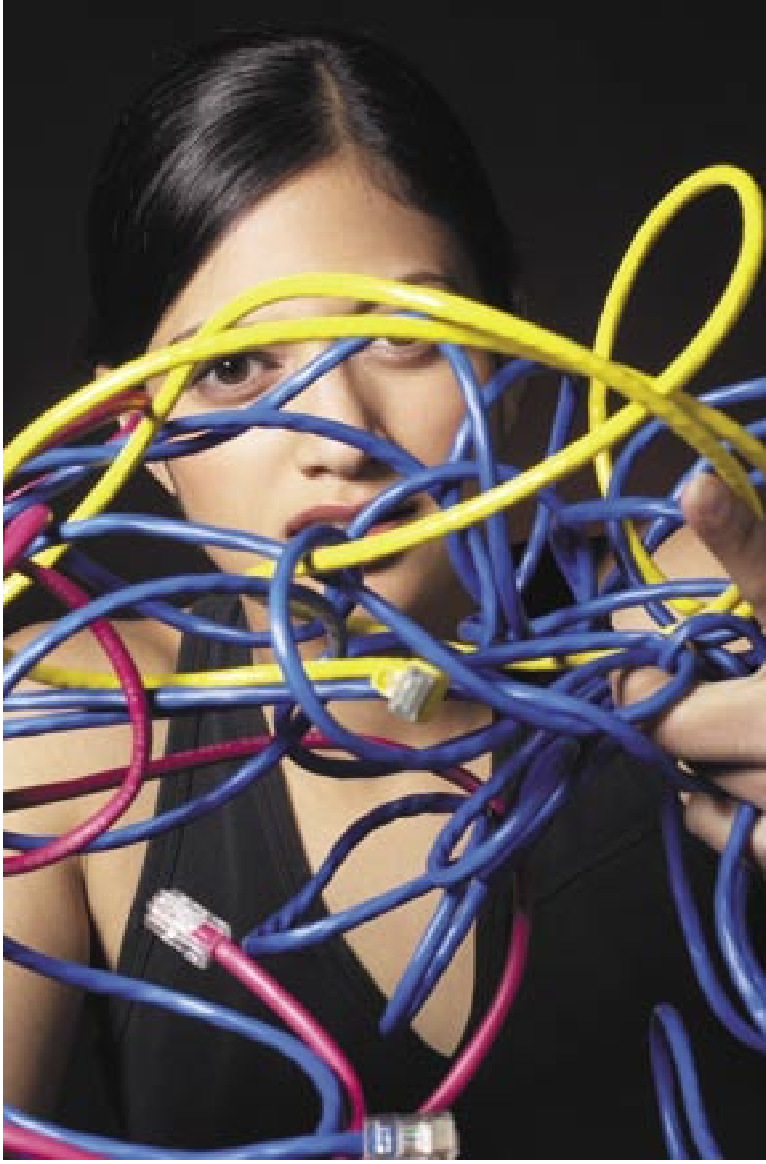
LOOMING LARGE:

The Future of Storage Security

SUPER SMART DEVICES

Security considerations for manager-free facilities

By Tim Seyfarth



Lately, there's increasing interest in creating self-storage facilities that offer 24/7 service—sites that operate without a manager or with reduced onsite staff. These automated facilities have their pros and cons.

On the positive side, they require less personnel, which means lower labor costs and fewer employee-related issues such as the need to hire, fire, train, settle disputes, etc. In addition, the lack of a manager's residence increases a facility's rentable square footage and eliminates the cost of apartment construction and maintenance. Automated sites allow for 24-hour access, which not only helps justify higher rents, but implies greater customer service and convenience. Finally, the ability to rent units around the clock means great revenue potential.

On the flip side, sites with minimal or no onsite staff face greater security challenges. First, the absence of consistent onsite management means fewer eyes observing facility activities. Second, while kiosk solutions can handle many manager duties, i.e. renting units and collecting payments, they can't do everything. To rent units, you need vacant spaces. If these are kept unlocked, they might be misused by other tenants, vandals or criminals. If they are locked, how do you allow tenants access to newly rented space? And how do you handle overlocks?

To successfully develop, market and protect a manager-less site, you must make the most of technological tools, "smart devices" that communicate with each other and your security system.

Electronic Door Locks

Kiosks make it possible for tenants to rent units, pay rent, procure a copy of their rental agreements, purchase tenant insurance and even buy locks for their units. On the security side, they can collect a tenant fingerprint, copy a driver's license and take a tenant's photograph. This is more than even a human manager will sometimes do in the course of a new rental. But there are things a kiosk cannot do, such as lock or unlock a unit—unless you use electronic door locks that tie into your management and security systems.

Electronic locks do not alter the conventional operation of a facility. A tenant still uses his own lock to secure his unit once the rental process is complete. What they allow, however, is the automatic unlocking of a unit when a new rental is made via a kiosk, and the locking of a unit if payment is delinquent or a tenant ends his lease.

Here's an example of how a system with electronic locks works: A new customer arrives at a facility at 2 a.m. and rents a unit using the kiosk. Upon completion of his rental, he receives a PIN code that he enters into the nearest access-control keypad. Three things happen simultaneously: the gate opens, his unit is unlocked, and his unit alarm is disabled.

A well-planned and designed electronic lock interfaces with your alarm and access systems, becoming an integral part of your site security. Not only does this integration reduce your overall security costs, it allows your electronic lock to be "smart," meaning it knows when a door is open, closed or something in between. It will not lock until the door is ready. It will also be able to report all changes in the state of the door as well as its current lock position to the site computer.

A Closed-Loop System

In a closed-loop system with acknowledgment features, all of your devices are smart—they can listen to your PC and answer it. In general, self-storage security systems use a method called "polling" to communicate with remote devices such as keypad access controllers and multiplexed alarm-system components. The PC sends a message to all remote devices, making a status request. In essence, it asks the devices if anything new has occurred since the last poll. The response could be that a gate code was entered, a door was opened, or a lock changed from locked to unlocked.

If action is required, the PC will send a command to the necessary device, and the device will confirm with a report of what it has done. Think of it this way: When two people converse, they acknowledge what they have heard from the other verbally or through body language. The same is true of a quality security system.

If only one end of the system has the ability to communicate, data loss is likely. For example, a door at your facility is opened. The alarm component monitoring the door detects the change in door state. In an open system, i.e., one that does not require a status report from all devices, the alarm will transmit the data to the PC, which is good. But because there's no back-and-forth communication, the alarm doesn't know if the data was properly and fully received by the PC. It deletes the message. If the PC didn't receive it, too bad, so sad. The door-opening event is lost forever, and no alarm sounds.

Using a true closed-loop system featuring acknowledgement codes at the remote-device and PC ends, data loss will never occur. The system is designed so the alarm component does not delete a change in door state until it receives the proper acknowledgement code from the PC. The ability to re-send the information is intact, and the data will be transmitted again during the next status request. The result is a truly secure system.

Communication Speed

Sometimes having smart devices isn't enough. For a security system to be truly successful, you must consider its speed of communication. For example, if you have 10 multiplexers and four keypads, a total of 14 devices must be continually polled by your PC. If a tenant comes to the entrance gate, he doesn't want to wait long for it to open. The faster the PC can communicate with the entry keypad—send its status request and receive the data (in this case, a PIN code)—the less time the tenant will wait. In the meantime, the other 13 devices need attention, since there may be doors opening or closing or a tenant at another keypad on the property.

When purchasing your security components, consider how long it takes to send and receive data between your PC and remote devices. Also consider how frequently the devices are "polled." The more frequently they are polled, the less time it will take for them to respond to an event, be it gate-code entry or a change in door status that yields an alarm. Your poll rate is the number of times per second your PC sends a status request to a device and receives an answer (one full cycle). Fast systems poll about 10 times or more per second. Faster is always better, so if your system exceeds this rate, you're in great shape.

By integrating kiosks, electronic door locks and smart devices with your access controllers and alarm systems—and meeting the need for speed—you can achieve an unmanned site that is monitored and truly secure. Make the most of smart devices, and get smarter in your day-to-day operation.

Tim Seyfarth is president of Phoenix-based Global Electronics Ltd., which provides gate-access controllers, alarm systems, electronic locks and Windows-based access/alarm-system software. For more information, call 602.437.8005; e-mail tjs@mail.global-electronics.com; visit www.global-electronics.com.