

September 30, 2005

APPLYING TECHNOLOGY

Technology Arrives To Allow Centrally Programmed, Keypad-Run Locks

Audit-trail reports are nice security feature – if there's time to consistently read them.

For some time now, industries that make widespread use of safes and vaults – including retail, banking, restaurants, hotels and casinos – have been converting from tumbler-style locks to keypad-controlled models. The next shoe is starting to drop as vendors ask security departments to buy into the idea of centralized programming and control of these safes and vaults over an IP connection.

This centralized administration lets companies program locks to accept a new employee's access code or deny a terminated employee's code, create an audit trail of usage and view exception reports of suspicious activity (for example, a safe door was left open for an unusually long period).

Among the vendors marketing the technology for centralized control is **Sargent and Greenleaf**/Nicholasville, Ky., which was recently acquired by **Stanley Security Solutions**/Indianapolis. A security administrator can, from a basic PC, run "centralized control across an enterprise of safe and vault locks," said **Phil Pitt**, marketing director for Sargent and Greenleaf.

Companies with 2,000 electronic locks might well conclude they cannot efficiently program and reprogram that many with proper security, Pitt said. "Now, you can do all of that remotely," he said.

Sargent and Greenleaf's system keeps an audit trail of lock activity to help security ascertain who accessed a safe or vault at what time, thereby narrowing the suspect list following a theft. The company also markets a \$999 software package to report exceptions activity and automatically send out alerts via e-mail or to a PDA or cell phone.

For example, if the company doesn't want a safe or vault door left open more than five minutes, it can have that standard programmed in as an exception.

The Sargent and Greenleaf system runs over a company's network, although lock keypads still can be operated manually if the network is down. The company sells its hardware – including an electronic lock, IP connection module and network card – for about \$1,500.

Navy Exchange Service Command/Virginia Beach, Va., a retailer for the military, is now upgrading from tumbler safes

to PIN-access models and already has converted some stores. However, the business is a long way from converting to networked safe and vault control, so **CS** asked **Joe Box**, corporate loss prevention and safety manager, for his thoughts on centralized administration.

What Box likes most about the technology as **CS** described it to him is the ability to create and maintain an audit trail of users. "You know which associates are going in and out of the safes," he noted. There's an automatic deterrent effect; if employees know the security department is monitoring them in this fashion, they are less likely to attempt to steal cash from the store safe.

Box also spots promise in the technology's ability to detect when safes have been left open for too long.

However, the downfall that Box sees in the Sargent and Greenleaf approach is, *somebody* has to monitor those activity reports if they're going to have any meaning – and that task "could be labor-intensive, depending on how many store safes you have." ☛

Contact Info: **Phil Pitt**, (859) 241-2223; **Joe Box**, (757) 440-4548.