

# IS YOUR BUILDING SECURITY WORKING AGAINST YOU?

BY MIKE JAGGER

In February 2006, the Vancouver Police Department received a call from a distraught woman who said she was being beaten by her husband and needed help. When police arrived at the downtown highrise where the call originated, they found the front doors locked and had to use the building's intercom to dial the suite. The phone was answered by a male who simply said, "she's fine" and hung up.

When the police tried to gain entry into the building by dialing other residents on the intercom, they learned that although any resident could buzz them into the front lobby, the security system was designed so that only a resident on the 18th floor could allow the elevator to open on that floor. For security reasons, none of the suite numbers were displayed on the intercom and as a result, the police were forced to choose between randomly dialing hundreds of residents to find one on the 18th floor or break into the stairwell and climb 18 stories.

This is not an uncommon occurrence for the police. In fact, it has become a big enough issue that the VPD created a program called "Project Access".

'Project Access' calls for construction companies and strata councils to install a lockbox, which would be accessible by the VPD Sergeant on duty. Inside the tube would be a full access key fob or card.

The fact that the police cannot quickly access a building in an emergency is clearly a huge problem and is only going to get worse. But lockboxes are not the solution. The Fire Department has used lockboxes for years and theft from these boxes has always been a major concern. Irrespective of construction and even if the box itself is monitored as a part of the alarm system, an external lockbox presents an unnecessary risk to condo owners.

If the lockbox gets broken into, a thief can gain full access to the building.

The best solution is remote management.

Remote management of building access control systems solve two very serious risks: 1) as described above, the difficulty for emergency responders to gain access to the building, and 2) it eliminates the risks associated with having an access control system managed through a PC located on-site and operated by a resident manager.

Rather than an access control system's database residing on a PC located at the client site (which in itself is a huge security risk), through remote management, the database is on a secure server located in a high-security, central monitoring station.

Using either dial-up or broadband connections, security firms (that have the proper infrastructure) are able to remotely manage the database, including adding, modifying or deleting users as well as make regular database back-ups.

With a fully managed system, off-site security can talk to the police, verify their identity, view them live on camera as well as remotely unlock the front door and control the elevator for them.

Another common failure of most building access control systems is the lack of professional management of the system. In most cases, the database that controls the system is 'managed' by a resident manager, concierge or other person for whom database management is not a full-time job. The result is often that new users get added into the system, but regular audits are not performed and many keyfobs and cards for former residents/tenants are left in the system. Further, because the system is being maintained on a single PC, the access control software is at significant risk of data loss due to hard drive failure, improper back-up procedures as well as the risk of the physical theft of the PC itself.

The fewer key fobs/cards in circulation, the better. Even more important, each and every key fob must be assigned to a single person to maximize accountability. Remote access control system management maximizes the effectiveness of any

system and ensures the fewest possible 'holes' in the building's security.

Rather than waiting until a serious incident occurs in your building, ask yourself the following questions:

1. Where is the database for your access control system physically located? Is it secure? Is it backed-up? How often?
2. Is entry to the parking garage tracked in the same way that entry through a door is? (ie. Do you know exactly who opened the garage door and when? Or does everyone have a generic 'clicker' that is not individually assigned?)
3. Does your building still use lockboxes for the Fire Department, or anyone else?
4. Is the building's telephone room secured with its own separate alarm system?
5. When was the last time you had a security professional provide a thorough audit of your building? ♦

*Michael Jagger is the founder and president of Provident Security, a full-service security firm based in Kerrisdale. Provident provides security guard, alarm installation, service, monitoring and guaranteed five-minute response to Vancouver clients. In addition, Provident provides remote access control management for clients throughout North America.*