Audits key to access control as third-party fob duplicates emerge

BY SCOTT HILL

Within the condominium industry, there has recently been concern about third-party suppliers that are duplicating fobs for owners. Most worrisome would be the lack of control that the condominium corporation can now exercise over the access within the facility.

Condominium corporations use fobs to control entry to their buildings for several reasons. Fobs provide information on who accessed the common element with a date and time stamp, which may be important in the event of a security incident. Fobs can also be deactivated without changing the building systems, whereas if a common key is lost, the board of directors must decide whether it's necessary to re-key the entire building. And with fob systems, boards of directors can schedule time restrictions on access to certain areas, such as the gym or party room.

There are several steps that a condominium corporation can take to address security breaches such as third-party fob duplicates and maintain proper access control within its building.

The first step would be education and governance. Property managers and boards of directors should communicate to the tenants and owners (resident and non-resident) that only fobs provided by the condominium corporation are to be used within the facility. If necessary, the board can pass a rule stating as much.

The second step would be to implement control procedures to ensure that this policy or rule is followed. When entering a fob into the system, or during an audit, it's possible to set up an authorization field within the database with an appropriate code. A recognized fob will have the correct information in this field, whereas a fob that is duplicated by a third-party supplier will not. The absence of this authorization code will alert building management that there is an unauthorized fob being used within the building.

Once a condominium corporation has policies and control procedures in place, most databases can be used to create custom reports that sort every time a fob was used by authorization code. A preview of this report will allow a property manager to quickly spot any abnormalities within the specified time range. The property manager can identify the unit/person that has an unauthorized control device by combining the date and time of the event with a review of the video surveillance system.

It is recommended that property managers run these reports weekly. It is also recommended that fob audits be conducted at least once a year to keep the database current. These audits can be timed to coincide with the annual general meeting (AGM) mail out for convenience.

What a fob audit does is ensure that the all the fobs in the database are registered to valid residents and owners within the condominium. These audits often reveal that databases have not been cleaned in years. Sometimes there are past owners in the system that moved out of the condominium years prior. In addition to taking up memory in the system, these fobs, and in some cases old remote controls for the parking garage, could pose a security risk if they are found and used years later.

When a fob audit takes place, each owner or resident of the condominium corporation must register all the fobs and remote controls that they have in their possession. This includes all control devices that have been provided to family and hired help, such as cleaning personnel or dog-walkers. Once all the access control devices have been registered as current, the database is then purged of all the old, and supposedly lost, access control devices. This way, the condominium manager can rest assured that only authorized residents may access the building.

These audits can be handled internally, but there may be some inherent risk in having inexperienced in-house personnel complete them. Usually the contractor who installed and maintains the directory board has the ability to conduct an audit. If this is the first audit that has been conducted in many years, the board of directors may want to consider bringing in a fresh pair of eyes to do the audit.

Whomever conducts the audit may recommend rules and/or procedures to implement based on its findings. For example, there should be a trigger in place that reminds property managers and/or superintendents to update the database any time there is a change of owners or tenants in the condominium corporation. Most condominium corporations require residents to fill out a form to book elevators for moves, so one way to do this would be to dedicate a section of this form to recording incoming and outgoing access control devices.

Putting in place proper policies and procedures for access control systems is one of the most important steps that a condominium corporation can take to protect its facility and those that dwell inside. In this, communication and follow up are key. Residents of the condominium must be informed that these policies are for the safety of all. Residents must also be told that there are proper controls in place to ensure adherence to the rules, including those relating to third-party fob duplication. □

Scott Hill of 3D Security Services has been a practicing RCM with ACMO since 2012, a Physical Security Professional (PSP) with ASIS and a Certified Security Project Manager (CSPM) with the Security Industry Association. 3D Security Services is an industry leader in physical facility security with a specialization in condominium security.