Business & Company Resource Center

a tad dated

Security Management, April 1995 v39 n4 p61(3)

Getting a lock on key control.

E. Floyd Phelps

Abstract: Key control is an important component of a security program. Since keys provide access to facilities, they make the company vulnerable to theft, vandalism and similar crimes. Security managers thus need to formulate a key control plan that identifies a key, its holder, the number of copies available and what it fits. The plan includes the company's key policy and the procedure to be taken in case of key loss.

Full Text: COPYRIGHT American Society for Industrial Security 1995
Final exams were just around the corner and Jack's grades were so bad that anything less than an A on the final would result in a failing grade for the class, one Jack needed for his engineering major. But Jack wasn't worried. He had a copy of the exam and all of the answers. Getting the test hadn't been as hard as he had anticipated. With little trouble, he had been able to obtain a key to the professor's office. After making sure he knew when the professor would be out, Jack simply walked in and took what he needed. The next day, Jack aced the test.

This serious breach of security almost went undetected. It was discovered only because the professor noticed that a few papers on his desk had been disturbed. He confronted Jack, who then confessed.

An incident much like this fictionalized account actually occurred at Southern Methodist University several years ago. Similar incidents are probably taking place and going undetected on many campuses and in many businesses each year. The cause is lax key controls.

Keys - whether they are access control cards, the number codes for an electronic punch pad, or the metal devices used to open mechanical locks - are the first line of defense and sometimes the last. Yet they are often handed out freely, left lying around an office, or lost. In each case, the organization that cannot account for all of its keys has lost some control over access to its facility. The result can be theft, vandalism, or worse.

One of the first goals of a company's security manager should be to develop a comprehensive key control program that tracks each key, who has it, and what it fits. No keys should be left unaccounted for or undocumented.

Accountability. A key control plan should start with an in-depth survey that identifies every door and lock at each facility a company owns or rents. The survey should include a listing of the keys that operate each door as well as the sensitivity level of each room. Each key should be numbered with the corresponding facility, door, and key holder (the employee assigned that key). For example, a key might be numbered AB-23-05. The AB would identify the facility, 23 would identify the doorflock, and 05 would be the copy assigned to the key holder.

The name of the company or facility should not be directly identified on the key. Some companies have their name stamped on each key in the hopes that it will be returned if it is lost. This only increases the company's vulnerability by telling the finder where to go.

A file should be maintained on each key that describes what the key fits, who holds it, and how many copies exist. All of this can be done manually, but a computer record can be much more efficient. Software systems designed especially for key records are available.

In selecting a computer program, security should first determine what needs to be tracked. For example, as discussed earlier, security managers should at a minimum keep a record of all key holders, the keys they have been given, and which doors those keys open. They may also want to show who is authorized to issue each key, when keys are used and where, and the maintenance schedule for each lock.

The program must be user-friendly and allow the key manager to cross reference records, which will enable security personnel to find and update records fast. It should also be able to run reports.

When purchasing software, the security manager should ask the following questions:

* Can key holders and their keys be sorted by department?

* How will lost keys be tracked?

* Does the software designer have a support telephone number to call if problems arise?

* Are there password capabilities?

Key distribution. The ideal method of key distribution is to have keys issued from one central office in which each authorized key holder must receive the key in person. When each key is issued to an employee, the transaction should take place in writing, with the key holder signing a form to verify receipt of a specific key. This document can also outline any regulations that accompany the privilege of carrying the key.

The company must determine who is authorized to order keys for employees. Those managers should be instructed to order only keys that are needed.

Training. Training is a big part of a key distribution program. It is imperative for managers to understand that keys are a tool to protect company assets and are not to be distributed freely to anyone who asks for a copy. Most people, unless instructed, will issue a key for convenience. Managers who are bothered several times by an employee to have a certain door opened will often issue the employee a key.

The manager gives up knowing whether the key has been duplicated by an unauthorized source and whether the pirated key has been given to another person. The supervisor also relinquishes the ability to know when the door is opened and for what purpose.

If a person needs to get into an area, its door should be opened and the activity witnessed by the person authorized to have access. The person who has an authorized key should make certain that the area is secure before leaving.

Policy. For these rules to work, they must be stated clearly in a written policy that stresses the importance of key control. The policy should detail what is expected of those who have company keys while also conveying the company's commitment to key control.

The policy statement gives a company the chance to decide how it will handle different situations. For example, the company must decide whether nonemployees, such as vendors, will receive keys.

Generally, keys should be assigned only to employees. The company has little control over people it does not employ. Rather than issue a key to a vendor, a better policy might be to have an employee meet the vendor and open the door at a prearranged time. If it is necessary to give a key to a vendor, the vendor should agree, in writing, to rekey the necessary locks if the key is lost.

The key policy should not be too restrictive or detailed. Some leeway should be left for necessary flexibility. For example, instead of saying that only company employees can be given keys, the policy should state that the security manager must approve the assignment of all keys. The security manager then has the ability to issue keys to other parties, such as contract guard services or landlords, as appropriate.

The fire department merits special treatment. An alarmed lock box that contains the master key to the facility can be placed on the outside of the building. The fire department can then use a key to the alarm box to get the building's master key in the event of an emergency when the facility is locked for the night or the weekend. The organization's security

department is notified when the alarm box is opened and can check to ensure that the master key has been returned.

Action plan. In addition to a key policy, the company should draft an action plan that outlines the procedure to be followed when a key is lost.

The plan should direct employees to report lost keys immediately. Management should always respond to lost key incidents by changing the compromised locks or invalidating the card code or employee keypad number.

If an employee is terminated or transferred, procedures should provide that security will be notified and that keys will be collected and returned to the security manager. If the keys are not returned, the locks affected should be changed.

Changing locks. The most efficient way to ensure the integrity of a mechanical lock system is to change the existing locks and issue new keys. A company should consider new locks if it has just relocated, is suffering from internal theft, or cannot account for all keys.

The most popular basic lock is the pin tumbler model, which is used on most doors. The lock's components include a cylinder, or lock housing; the core, a round rotating portion that fits inside the cylinder and contains the keyway; and pin tumblers, circular pins within the lock cylinder and core. When a door is locked, the tumbler pins rest inside corresponding holes that prevent the core from rotating and releasing the bolt. The proper key raises the pins out of those holes, thus allowing the core to turn and open the lock.

While these locks have been around for years, there are various options on the market today that can make a locking system more secure.

When shopping for new locks, security managers should consider different options, including restricted keyways, removable cores, block-out cylinders, and replacement cylinders.

Restricted keyways. The first thing a security manager should consider is installing locks with restricted keyways, a system that uses key blanks that are not on the open market. These keys cost a little more, but they protect the company against the unauthorized duplication of keys that can then be lost or distributed to people outside the company.

With this type of system, the company buys all of its keys directly from the manufacturer or from the manufacturer's designated locksmith. The locksmith, usually located near the company that purchased the new locks, is the only one authorized to make a particular key. In other cases, an organization that installs restricted keyways can cut its own keys after buying the cutting machine from the key manufacturer, usually at a cost

of about $5,000.

Removable cores. Another option that can be used with or without restricted keyways is the removable core. Locks at an entire facility can be changed quickly by removing one core with a special key and replacing it with the new one. This system allows a company to change locks at a remote site without a locksmith. However, the change key that removes the cores is equivalent to a master key and must be protected.

Block-out cylinders. Unauthorized, after-hours entry by individuals with keys can be prevented by the use of a block-out cylinder. This is accomplished by a special master key that places the locking device into a secondary position, preventing all other keys from operating the lock.

This system does have its limitations in that the person with the special key must be there at all times to secure and unlock the system.

The block-out cylinder is not available with every lock system. Security managers who think they may eventually want this feature should research whether the locks they are buying now can be upgraded later.

Replacement cylinders. In addition, many companies are retrofitting their existing locking system by purchasing replacement cylinders designed by manufacturers to fit the locking devices of the major lock companies. Restricted key-ways can be used in this case too, allowing a company to completely rekey using existing locks.

An organization must also decide whether it will install a lock system that relies on one grand master key or several master keys. For example, a university or hospital complex might want only one grand master key that can gain entrance to every building on its campus, or it might opt for several different masters that can each open only the doors of one building.

In the past, many organizations installed systems that required one master key, but the trend is now toward smaller, self-contained key systems. The reason for this is simple. By using several masters, an organization has to rekey only one building if the facility's master key is lost.

There are several other issues to consider when buying new keys and locks, including the durability of the lock and the responsiveness of the manufacturer in shipping the merchandise and resolving problems.

Access cards. In addition to the traditional mechanical locking system, organizations can also consider using a computerized card and card reader system. Access control cards have several advantages. They allow a company to electronically record who is entering a building and at what time. Lost cards can be removed from the system so that they will not work if found by someone else. However, a card will not overcome the

problems of piggybacking, where someone who does not have a card enters behind a person who does by grabbing the door before it closes. It also does not necessarily stop someone from using a card assigned to another person.

Card access systems are also expensive to install because of the cost of the cards, computer equipment, software, readers, and setup.

Punch pads. Punch pads, both mechanical and electronic, can be used in situations with high staff turnover. Codes are changed more easily than traditional locks.

Both access cards and punch pads allow companies to regulate entry into the facility based on the time of day.

Preventing abuse. A comprehensive and consistently enforced key control program can only go so far. Other measures are needed to supplement these policies.

To prevent someone from gaining entry by simply removing exposed hinges, hinges should be installed on the inside of interior doors, and "fixed pen" hinges should be used on exterior doors.

Exterior locks should be flush mount (mortise or rim) lock sets, which are harder to defeat. Windows on the first floor should be kept to a minimum or installed in a narrow design to prevent entry. Back-up by an alarm system is also a way to detect unauthorized entry.

To assure that all doors are closed and locked, security officers must monitor entrances and exits either physically or through a central monitoring station.

Employees must be able to get into the building and into their workstations as required, but a company must also protect its assets. A good key control program with a locking system that fits an organization's needs can provide a strong defense.

E. Floyd Phelps, CPP, is assistant director of the Department of Public Safety at Southern Methodist University. He is a member of ASIS.

Bus. Coll.: 85Z2516

Article A17021258

THOMSON GALE © 2003 by The Gale Group, Inc.