# Business & Company Resource Center

*Security Management*, August 1998 v42 n8 p67(4)

**Lock in a good key policy.**

(additional security using mechanical locks)
*Charles Cameron*

**Abstract:** The use of electronic security systems must not ignore the significance of mechanical locks which provide additional security. Mechanical locks cost less than electronic control systems but are proven to be as effective as their electronic counterpart. The factors that must be considered when planning to use mechanical locks for facility security are inventory of locking units, corporate operational requirements, key identification and monitoring, key control policy, key system hierarchy and prevention of unauthorized key duplication.


There is no question that electronic locks offer many benefits to a corporate security operation. Stolen access cards can be easily deactivated and rendered useless, electronic audit trails can tell investigators who entered a facility at the time of a crime, and doors can be locked from remote central stations. But in the rush to purchase electronic access control security managers should not forget about the company's mechanical locks - most of which will remain the primary protective measure in a building even after a high-tech system has been installed.

Mechanical locks cost significantly less than their electronic counterparts. While a company can expect to pay $700 or more per door for an electronic lock, the existing mechanical lock can be upgraded with a new key cylinder for about $30 to $60 per door. Because of this price differential, many companies purchase electronic systems on a limited basis, using them for high-security applications while relying on mechanical systems for the rest of the building. As such, the security professional must develop a program to manage the company's mechanical key system.

The security manager should follow several steps when establishing and managing a mechanical key system: inventory the corporate facility to identify the number and types of locks in the building; determine the operational needs of employees; and establish policy and procedures for key distribution.

Inventory. The first step is for the security manager to inventory all locking units in the corporate facility. The inventory should be carried out

by someone with a knowledge of lock systems, such as a locksmith, or a member of either the security department or the facility management department (or both). Locks should be counted on a floor-by-floor basis, with the floor tallies compiled for each building and then the building tallies compiled. The inventory defines the size of the mechanical lock system and yields information that will help determine how the system should be managed.

In addition to counting the locks, the security manager (or whoever is handling the inventory) should collect data on the manufacturer and model of the lock at each door. Different model locks require different types of cylinders, and cylinder types can also vary by manufacturer. This information will be important when ordering new cylinders if the company needs to convert the existing locks to a new key system.

The person collecting the lock data should also physically label each door with a number (either in a visible or concealed location) so that lock hardware and keying can be specified correctly for each door. This information should then be retained in a database as an aid in maintaining and servicing the key system and door hardware.

A common labeling mistake is to use the room number for identification - that can create confusion when there is more than one door associated with a given room number. It's better to assign one number per door.

Operational needs. After taking an inventory of the lock systems, the security manager must define the operational needs of the company's employees and support services and determine whether the existing key system meets those needs.

Location of company departments is one factor to be considered. A multistory building, for instance, may have been equipped with one master key for all locks in the building and submasters for each floor. While this arrangement appears to make sense on the surface, it would create problems if two departments share the same floor and the department managers each seek a separate master key for their own department's space.

Security and life-safety response operations should also be reviewed. For example, if there are ten buildings on a corporate campus, each with its own master key, security supervisors and emergency response personnel would require a ring of ten different keys to access those buildings during an emergency. The security manager, working with senior executives, must decide whether this is an acceptable number of keys for safety personnel to carry with them - or whether a consolidated key system would be more effective.

The structure of maintenance operations and housekeeping assignments is also important to consider, especially in the hotel business. Are

maintenance personnel permitted to have unsupervised access to all areas, including offices, or just the mechanical rooms, electrical closets, and utility areas? Are housekeepers responsible for an entire building or a specific area, such as a floor or a wing? The goal is to provide a minimum number of keys at the lowest master key level practical to allow the cleaning staff access to their assigned areas.

Policies. Now the security team is ready to develop a key management policy. Good key control begins with a well-conceived policy. This document is a general statement that describes the goals of the organization and outlines the basic rules that employees must follow when using company keys.

The policy defines expectations and areas of responsibility, both for those who issue keys and those who receive them. For instance, a typical policy might read as follows: "In order to protect the assets of the XYZ Company, the security department is responsible for the design, maintenance, and administration of all company locks and keys."

The policy might go on to explain that keys are the property of the company; that employees who are issued keys are responsible for safeguarding them and prohibited from duplicating them; and that service personnel (maintenance and housekeeping) may be issued master keys of various levels so that they can perform their duties. In addition, a policy might outline the basic responsibilities of the security department, saying, for instance, that "security is responsible for issuing keys to authorized personnel, maintaining all key records, and ensuring that the locks are maintained and rekeyed to the company's key system standards."

The policy, which is usually about two or three pages long, should be supported by a more detailed set of procedures or regulations. This second document establishes the day-to-day rules that the security department will follow to meet the goals and statements outlined in the key control policy. For example, while the policy might state that the security department is charged with issuing keys to employees, the procedures would spell out the specific steps employees must take to get a key - such as filling out a request form, providing proper identification, and getting approval from supervisors.

Keeping the policy separate from the procedures gives the company more flexibility when changes must be made in the key program. For instance, if the company wants to modify the request form or any other requirements, it only needs to change the procedures rather than issuing a new policy statement.

A company with a strong policy has better control over its keys, which results in fewer keys being lost or compromised. Therefore, a good management policy and set of procedures help maintain a system for a

longer useful life.

Key hierarchy. If the company is putting in a new key system or upgrading an existing one, security personnel should first determine the key system hierarchy. The key system hierarchy establishes the size of master key groups as well as the number and levels of master keys needed.

The hierarchy design is developed using the building inventory and operational needs information. The security manager should obtain assistance on this step from a locksmith or architectural hardware consultant with experience designing large multilevel master key systems to ensure the development of a professionally designed key system appropriate to the company's needs.

The key hierarchy is important in defining the implementation plan for the system. If management wants a separate master key that will access only building entrances, it needs to be planned into the system from the beginning. Trying to implement such a change after some of the buildings have been keyed into the system usually requires redesigning the key system and rekeying the locks affected by the design change. In addition, a good rule of thumb is to design the system for up to 200 percent expansion to allow for new facilities and rekeying within the system.

Key tracking. All keys should be uniquely marked with a serial number that allows the security department to identify and track each key. Keys may be either issued for long-term use or checked out for temporary use, depending on the situation. The security manager should develop record keeping forms and procedures to document all key transactions. Even keys that are issued for long-term use should have a renewable issue period, usually one or more years.

Master keys must be treated with special care and require additional control procedures. Only authorized personnel should be permitted to access master keys; they should never be carried off site; they should be stored in a secure cabinet when not in use; and they should be accounted for when removed and returned.

There are several mechanisms that can be used to control the distribution of keys, including a staffed sign-out station, an electronic recording key cabinet, a mechanical tracking key cabinet, or an interlock device. These systems can be used to secure individual keys or a group of keys on a sealed, tamper-resistant ring.

An electronic recording key cabinet requires a key and a personal identification number (PIN) to release the required key or ring of keys. The unit can be programmed to restrict access to keys, such as by time of day, based on the PIN used. The electronic feature allows the security manager to track key use by employee, keys used, time removed, and time

returned.

Mechanical tracking key cabinets and interlock devices work in a similar fashion to the electronic system, although no PIN is required and no audit history provided. In this case, either a serialized access peg or an interlock key is used to release the desired set of keys. The key or peg is retained in the mechanism until the original set of keys is returned. An access peg will release any set of keys available in the mechanical tracking key cabinet, while the interlock key (used in the interlock device) can be set to release only specific keys.

Software options. Computerization of a key system's information is essential for efficient and accurate record keeping in large key systems. Many different software packages are available. While each program's features may differ, the basic software package allows a company to keep records regarding each key, the doors it opens, and who has it at any point in time. The software will alert security personnel when a key is overdue.

Most of these programs have passwords with different levels of protection. Some packages allow the security manager to digitally store an employee's photograph in a searchable database, which allows security personnel to verify the identity of an employee who is signing out a key.

Another common feature is the printed key receipt, in which the computer generates a written document, or "receipt," that specifies the key number that was signed out, the employee who took the key, and the time and day the key was checked out. The security manager can require that the employee sign the receipt, which serves as a written record of the key transaction.

Some programs also keep more detailed records about each lock, such as the location of the lock as well as the lock's brand name, type, finish, and maintenance schedule. Others can keep information about a key's bitting information and lock pinning calculations.

These programs range in price from $400 to $1,800, depending on the number of records that can be maintained and the other features offered. Three sources to check for software are Key Records Manager (KRM) by Locksoft Inc. (402/461-0201), Lockup by Security People, Inc. (800/989-0201), and KEYMAN by MANAGEWARE (818/346-9606).

Most of these types of programs are Windows based, including Lockup and KEYMAN. (Key Records Manager is a DOS-based program, although a Windows version is due out by the end of the year.)

Many vendors offer demo products that a company can use before committing to a purchase. The security manager should test the program by inputting data from a small portion of the company's locking system to become familiar with the software. Such a trial period often reveals a

need for data formatting modifications or changes in procedures. If the in-house staff lacks the expertise, the company may want to call in a consultant who can provide training in data collection and formatting and can tutor staff on the use of the key management software.

When a program has been purchased, the security manager must input information consistently if the data is to be useful. For example, some programs do not clearly explain the need to pad numerical data with zeros to obtain better organized and more useful reports. For example, instead of inputting numbers as "1, 2, or 11," the security manager might have to input the data as "0001, 0002, and 0011." Building names or numbers must be consistent, and personnel must edit the work carefully to avoid typos and other mistakes that can make it difficult to retrieve data later.

Enhanced security. An important component of a managed key system is the prevention of unauthorized duplicate keys through the use of patent-protected keys. Patent-protected keys are controlled by restricted distribution of the patented key blanks. The blanks are issued only to the company that purchased the system - they cannot be found in hardware stores or other places where key copies are made. Patent-protected keys can cost three times more than standard key blanks. Patent-protected keys fit in their own patent-protected cylinders or high-security cylinders.

As an added protection, the security manager should also consider using high-security cylinders in certain locations. These cylinders help guard against unauthorized entry through manipulation of the lock's tumblers - known as picking a lock - and are also resistant to drilling. High-security cylinders can cost up to two times as much as standard cylinders.

Maintaining the performance and integrity of a key system requires servicing the locks and cylinders according to the manufacturer's specifications and procedures. Any service work on a key system must be performed by a locksmith with training and experience appropriate to the particular key systems. The use of untrained personnel who are unfamiliar with a system and its structure can lead to key interchanges or other problems that reduce the security, effectiveness, and useful life of the system.

The key to better access control and an improved bottom line need not lie solely in new technology. By creating a well-conceived key management system, a security manager can both increase security and extend the life of the system from the normal five years to as long as twenty-five years - locking out trouble and locking in a good return on management's mechanical key system investment.

RELATED ARTICLE: KEY CONTROL CHECKLIST

* Inventory the facility, noting the manufacturer and model of each lock.

* Physically label each door with an ID number.

* Determine whether the system meets current needs.

* Review life-safety response as it relates to key accessibility.

* Review key use and control for maintenance and housekeeping purposes.

* Develop a key control policy and detailed procedures that explain the specific steps employees must follow when receiving or returning keys.

* Uniquely mark all keys.

* Document all key transactions.

* Control distribution with logs or devices, such as an electronic recording key cabinet.

* Treat master keys with special care.

* Consider patent-protected keys or high-security cylinders to prevent unauthorized key duplication or lock picking.

* If upgrading or redesigning, determine the key system hierarchy (how many master keys and levels) before installing a new system.

* Build in the potential for up to 200 percent growth.

Charles Cameron, CML (certified master locksmith), is the lockshop manager at The University of North Carolina at Greensboro. He is a member of ASIS.
**Bus. Coll.:** 110X1554

Article A21060477