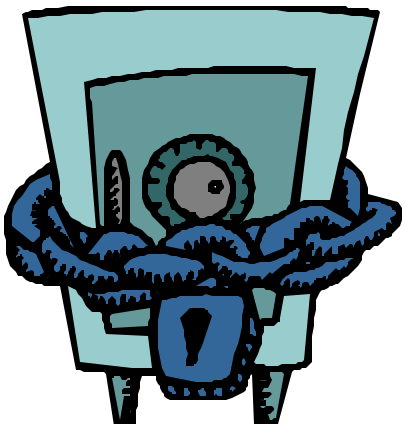
SECURITY REQUIREMENTS AND CURRENT TECHNOLOGIES FOR COLLECTIONS STORAGE

By Steven R. Keller, CPP

Contributing Author: Darrell Willson, CPP Deputy Administrator National Gallery of Art Washington, D.C.



There are three major elements to good museum security. They apply to the security for collections in storage as well. The three elements are "access control," "parcel control," and "internal security." If properly applied, good security can be achieved without bringing curatorial operations to a grinding halt.

Museum collections are at their most vulnerable when they are in storage. "Out of sight, out of mind," or so the old saying goes. It's true. An object missing from display will be noticed relatively quickly, or so we hope, but an object stolen from storage may not be discovered missing for decades. The speed of recovery is often directly related to the speed of discovery. The fact that an object will be noticed missing and will presumably lead to an intensive investigation while the trail is still hot serves as a deterrent to internal theft.

This leads us to the value of prevention. If you can control who comes and goes (administrative vs. curatorial employees, visitors, contractors); where they go once inside (galleries, offices, collection storage vaults), and when they are permitted to enter (day, night, weekends, holidays, etc.); what they carry in (razor blades and spray paint), and what they carry out (items from the collection, computers, money), and if you can hire only honest employees and keep them honest, you will achieve perfect museum security.

Museum storage rooms need to be accessible. The museum storage vault is not an attic, where one ventures only when one must and the rest of the time gathers dust. Modern museums have important objects in storage at any given time, and collection storage is often used for active study and research. So, the first rule in designing security for collections storage is to keep things simple. If security makes access too difficult or inconvenient, it won't be used, or museum management and staff will find ways to bypass security. While it may seem that my recommendations are extravagant,

Steve Keller is a security consultant specializing in museums, cultural institutions and historic sites with headquarters at
555 Granada Blvd.
Suite G-3
Ormond Beach, Florida
32174
Tel. (386) 673-5034
Fax. (386) 673-5208
E-Mail steve@stevekeller.com

You may use this material for your own use, but please retain the copyright notice.
Copyright 1989, 1994 by Steven R Keller and Associates, Inc. All Rights Reserved

much thought has gone into making things as simple as possible. Those charged with preserving collections think nothing of spending precious funds and taking extraordinary steps to control temperature and humidity, and to protect collections from acid in paper or deterioration from light. We in security take our responsibility just as seriously, but often find that professional staff ignore our safeguards because they are slightly inconvenienced.

One of the principles of security for any facility is to provide only the access that is needed to collection bearing areas. This can be done best by compartmenting the contents of collection storage in such a way as to isolate certain items from certain other items, so that a person needing access to, say, large stuffed birds, won't have access to small gold trinkets. Exactly how this is done depends upon the workstyle and infrastructure of the institution, but thought should be given to subdividing storage into compartments. The greater the access to the collection, the greater the risk. The more we can divide the collection into smaller units, the more access to any one unit we can give to specific staff members and still retain a high level of security. It also will be more convenient for the staff members.

Each compartment can be secured according to the value, vulnerability, and importance of its contents. Compartmenting can be by curatorial department and within that, by value or vulnerability of the various objects. Small gold trinkets should be secured behind solid walls, while large stuffed birds may be able to sit openly on shelves behind mesh screens. When determining the method of securing each type of material, include the security director or security consultant, since they often have an entirely different perspective on what is vulnerable based upon their understanding of how goods are converted to cash on the street. When asked to assess the vulnerability of objects in one art museum collection as part of an exercise to test this theory, security professionals selected the gold jewelry as most likely to be stolen, while curatorial personnel selected a particular artist's paintings. The first object stolen after the survey was conducted was a gold pocket watch. Crooks are not connoisseurs. They steal what can be converted to cash most easily.

The storage room itself should be physically secure. How secure depends upon how vulnerable the contents are. Walls must be solid, preferably masonry, and resistant to the spread of fire. Most often, walls are of block construction with a minimum four hour fire rating. If high-value objects are stored inside, additional security should be provided by safes and vaults located inside the perimeter walls. Doors need to be solid, preferably hollow core metal or better. Collection storage rooms should be windowless. Walls should rise to the slab above, preventing someone from climbing over by removing suspended ceilings. If contents merit, walls may have to be fortified with reinforcing rods and grouting. The floor and ceiling slabs need to be equally strong.

You may use this material for your own use, but please retain the copyright notice.
Copyright 1989, 1994 by Steven R Keller and Associates, Inc. All Rights Reserved

Door hardware should be appropriate for the contents as well. In all cases, collection storage doors must be equipped with a high security deadbolt lock with a proprietary keyway, that is, one whose key can't be copied at a locksmith without the consent of museum management. Such systems are common for high security applications. Doors should be equipped with door closers, and hinges should be on the inside where they can't be tampered with. If hinges are on the outside, they need to be "pinned" so that they can't be removed and the door taken off.

The best way to enforce access control in collection storage besides having a guard assigned to the door is to equip the doors with card readers. Card readers use card keys, like your bank ATM card, that are programmed with information about the cardholder. Any given card can be programmed for access to any given door during any given time period-- hour of the day or day of the week. Cards even can be programmed to expire after a certain date. Thus, students and visiting scholars who must have access can be given a card key that expires if not turned in by the end of the semester or some predetermined date. Card readers collect data on who has entered and when they entered and store that information in a database, creating a paper trail. Besides providing a high level of access to those needing it and effectively restricting it for those not needing it, card readers are a deterrent to theft. It should be necessary to possess both a high security metal key and a key card to enter collection storage rooms. The metal key unlocks the deadbolt lock, and the card key releases an electric lock and records access data.

Storage rooms need to be secured with electronic burglar and fire detection systems. Smoke detectors should detect any early articles of combustion and signal the alarm early enough to permit action before the fire spreads. All doors must be alarmed to detect opening. This is done by installing magnetic contacts on every perimeter door and window. Any air duct entering collection storage must be physically secured with bars blocking the duct and alarmed to detect access via the duct. Within the space, motion detection, preferably infrared technology or "dual technology" employing both infrared and microwave technologies, should detect any movement anywhere within the collection storage room. It should be impossible to take more than two steps anywhere within the room without being detected.

Ideally, collection storage rooms will be protected with closed circuit television viewed by guards. Activity on the cameras should be recorded on time-lapse video cassette recorders, and any alarm occurring in the space, as well as any invalid card inserted into the reader, should be recorded automatically using what is called "alarm call-up." Many museums record employees entering and leaving the storage room, as well as activity within the space. State of the art access control systems using card readers have the photo of the card holder

You may use this material for your own use, but please retain the copyright notice.
Copyright 1989, 1994 by Steven R Keller and Associates, Inc. All Rights Reserved

programmed in the database. When the card is inserted, not only does the computer decide if access should be granted, the photo of the card holder appears on their screen in the control room. The guard is able to compare the image from the card to the live image of the person at the door and provide access if warranted. This prevents a duress situation where an employee is forced to enter the space by an armed criminal. Some museums provide keypads at the card reader so that a metal key, a valid keycard, and a secret personal identification number are required. This further protects employees from duress by allowing them to input their PIN number plus a duress code to call for help. Even though keycards can be programmed out of the system if lost, they can be used if the employee doesn't know he/she has lost the card. A keypad protects the keycard from being used if it is found before it is programmed out of the system.

Modern security systems also can monitor environmental conditions such as water leaks. It is not uncommon for the burglar alarm system to also monitor water sensors on floors and ceilings in storage areas.

Access to collection storage must be limited to those truly needing access. Board of Trustee members and other VIP's should not have access to storage without a curatorial or registrar's escort. In many museums, no one has access to storage except the registrar and/or the curator. Custodial activity must occur only with an escort. Junior staff, like student interns, should not be assigned to work in storage without a senior escort, and volunteers should never be given unescorted access. Building engineers must be restricted even if they insist on having rapid access in an emergency, unless you can remain in charge of those emergency access events.

It is important that security and engineering personnel have the ability to enter collection storage areas rapidly, but not without their superiors knowing about the entry. If guards can activate lights without entering and if collection storage rooms have CCTV cameras, guards can view conditions without actually entering. When an alarm occurs and access must be gained, guards should obtain the key from an armored keybox such as the Knox Box (TM). Knox Box (TM) is a trade name for one brand of armored, alarmed keyboxes. Guards carry keys to the keybox on their patrol ring. Opening the box gives them access to storage room keys and also signals an alarm to an outside central station, which has instructions to notify museum management. This prevents misuse of collection storage keys and gives the guard rapid access when needed.

Recently, the Museum, Library and Archive Committee of the American Society for Industrial Security, the primary professional association for security professionals, issued a document entitled "The Suggested Guidelines in Museum Security." This document is available from the American Society for Industrial Security, Arlington, Virginia, or the American Association of Museums, Washington,

You may use this material for your own use, but please retain the copyright notice.
Copyright 1989, 1994 by Steven R Keller and Associates, Inc. All Rights Reserved

D.C. It consists of approximately 120 individual requirements for good security that should be found in every museum. One of those provisions requires that a policy be in force, limiting access to storage for educational classes, to instances where adequate escorts are present to provide protection. It is no longer acceptable to permit one instructor to oversee 30 students in collection storage during a field trip, or for a docent to conduct tours of storage for museum visitors.

Access control involves restricting access to collection storage to those needing it and then only during hours of the day or days of the week that security can be maintained. Access is enforced by locks and hardware as well as by physical barriers. Alarms alert security personnel to breaches. Card readers are a more secure and foolproof method of providing access. Compartmentation within storage provides a better level of security when a large number of people must have access, and allows low-value items to be available to more people, while higher value items remain off limits.

Parcel control involves the removal of any "parcel," or material, from the protected space. It is maintained by limiting access to those who can be trusted, by making it difficult to remove something without being detected, and by creating a trail that identifies suspects if a theft occurs.

Internal security involves hiring only honest people and keeping them honest. Once honest people are identified and the need to be in collection storage has been established, they can be given access. To keep them honest, we provide audit and paper trails to enable us to prove who had the opportunity to commit the crime, and who was in collection storage when it occurred. The deterrent value of paper trails should not be overlooked.

Proper storage room design can help keep security costs low. The more entrances there are, the more it will cost to provide electronic security. The more risks that exist in collection storage (i.e. water pipes), the more costly it will be to secure the space against damage from the malfunctioning of those systems.

While it is the responsibility of the security system designer to respond to the needs of the curatorial staff and not the responsibility of the curatorial staff to design a storage room solely for security, compromise will assure a cost-effective protection plan. Security problems won't go away, so security should be addressed by all involved. It may be possible to design the physical space in such a way as to keep security costs low and minimize inconvenience to staff.

One example of a good security design is a collection storage room that is located immediately adjacent to the main guard office. Many museums place the guard control room on the loading dock so the guard can also control access at this critical point. The employee entrance is then designated as being via this door. Trash removal can be monitored as can deliveries of

You may use this material for your own use, but please retain the copyright notice.
Copyright 1989, 1994 by Steven R Keller and Associates, Inc. All Rights Reserved

goods and arrival and departure of staff. Imagine if the collection storage room entrance was also situated so that it could be constantly viewed by the guard in the control room. Access could be controlled and any objects of a significant size removed from the room could be observed. Honest employees will remain honest if they know that their movements in and out of storage will be under the watchful eye of a guard.

Another common problem with storage room design is the lack of a study space for scholars. Too often, visiting scholars are taken to storage and given several items to study. Staff members can't be tied up all day however, so the visitor is allowed to remain in the storage room unattended among the stuffed birds and gold trinkets. This situation could be avoided if there was a screened-off study area where collection materials could be brought. The visitor could have access to the one or two pieces delivered to the study area but not to all of collection storage. The guard could view the study room via a window and a CCTV camera.

Such a design also facilitates a "two key" access policy practiced by some larger institutions. Some issue a key to collection storage to the curatorial staff and a key to the security office. Access can be obtained only when both keys are used, making it necessary for a curator to report to the security control room, sign out the second key, and enter using his/her key and key card. Similarly, building engineers needing routine access must come to the curator or registrar for entry.

All of the above improvements will yield a secure collection in storage, but none is truly effective if the security staff is not well trained and the electronics are not well designed. If an alarm occurs but is not transmitted to the central monitoring station because a wire was cut and the breach went undetected, no security really exists. Any effort to secure items in storage must include a plan to properly administer the security program in full.

The collection need not be at its most vulnerable while in storage. Artifacts and specimens can be well protected if security is given a sufficiently high priority by museum management. A knowledgeable security system designer can assure that security can be achieved without being obtained at the expense of convenience and productivity of curatorial staff. Modern technology enables a minimal guard force to electronically secure high-value assets in storage for a relatively low cost. But the most important step is the development of a comprehensive policy to control access, account for parcels being removed, and monitor employees to keep them honest. The first step is to obtain a copy of "The Suggested Guidelines in Museum Security."

DEFINITIONS:

access control: The process of controlling who comes and goes, when they may come and go, and

You may use this material for your own use, but please retain the copyright notice.
Copyright 1989, 1994 by Steven R Keller and Associates, Inc. All Rights Reserved

where they may go once inside. Access control occurs at the outer perimeter of a building and again at various other interior perimeters, such as the dividing point between public areas and employee areas and at the dividing point between low-security areas and high-security areas.

parcel control: The process of controlling what is carried into a museum and what is carried out. It can occur at dividing points between low-security areas and high-security areas such as a storage room doors.

internal security: The process of hiring only honest employees and keeping them honest. It is done primarily through pre-employment screening and through creating accountability such as audit trails. Not only do they keep honest employees honest, audit trails allow honest employees to be free of suspicion.

proprietary keyway: The keyway is the series of grooves on the side of a key that, when they match the grooves in the cylinder, allows the key to slide into the cylinder. Once inside, the "cuts" in the top of the key must fit the interior of the cylinder for the key to turn. A keyway is "non-proprietary" when the key blank contains a configuration that is relatively common and the key blanks can be purchased at most hardware stores and locksmiths. A keyway is "proprietary" when it is reserved for one customer, such as a museum, and blanks can be purchased only at one distributor and only with a pre-arranged procedure to authorize that purchase. This prevents employees from taking their properly-issued or properly-loaned key and having a copy made which they can use after hours or after they leave the museum's employment.

card reader: Computer-based access control systems are systems that use a series of electronic locks operated by card keys accessed via cardreaders. Think of your ATM card as a key card that works with the ATM, a card reader. Key cards are encoded with data. Access control systems can be programmed to grant access during specific hours of the day or days of the week for each individual person. Card keys can be programmed out of the system with a keystroke on the computer.

key card: See "card reader."

magnetic contact: Magnetic contacts are alarm switches that detect the opening of a door or removal of a hatch. They interface with a burglar alarm system.

motion detector: Some motion detectors "see" invisible infrared radiation given off by all living things. They see a fixed pattern of infrared temperature. When an intruder moves across the pattern, the established pattern is disrupted by the increased heat of the moving body, and the signal is sent to the alarm system. Some motion detectors send out a signal (like police radar) and when a moving body disrupts that pattern, this is interpreted as motion and the alarm is activated.

LITERATURE CITED: Museum, Library and Archive Committee of the American Society for Industrial Security,

You may use this material for your own use, but please retain the copyright notice.
Copyright 1989, 1994 by Steven R Keller and Associates, Inc. All Rights Reserved

1989. "The Suggested Guidelines in Museum Security," 1989, The American Society for Industrial Security, Arlington, VA.

You may use this material for your own use, but please retain the copyright notice.
Copyright 1989, 1994 by Steven R Keller and Associates, Inc. All Rights Reserved