Collection Security

RICHARD W. BOSS

COLLECTION SECURITY HAS always been a concern of librarians, but recent publicity about major thefts and vandalism has sharpened interest in the development of a systematic approach to the problem. The most famous case is probably that of James Shinn, who allegedly stole rare books valued at some $500,000 from colleges and universities around the country before his arrest in 1982. In the same year Thomas Freeman, a former Princeton student, was arrested on charges of stealing more than 3000 books from the open shelves of more than a dozen libraries in New Jersey. Only a short time later, some 5600 books were recovered from the apartment of Glenn Swartz in Los Angeles, most of them from the open shelves of Los Angeles Public Library's Central Library.

Book theft is only one serious security concern of libraries. In the period from 1972 to 1980 there were at least thirty-two reported incidents in which fires were set in locations ranging from book returns and mail slots to bookstacks. Of the sixteen arsonists who were apprehended, two were library employees. In 1982, an arsonist set fire to the Hollywood Branch of the Los Angeles Public Library and caused some $3.5 million in damage, including the destruction of more than 65,000 volumes. Other forms of vandalism are generally not as well documented as fires, but their incidence is even greater.

Richard W. Boss is senior consultant, Information Systems Consultants, Bethesda, Maryland.

Losses

While there has been no national inventory to determine the extent of losses suffered by the nation's libraries from theft and vandalism, estimates range as high as $250 million a year. Individual institutions have reported collection loss rates of 3 percent and more per year. When this is compared with gross acquisition rates of 5 percent or less per year, the effect is staggering. Even worse, the thieves have the advantage of being able to steal the best of the selections made by librarians. Loss from arson and other forms of vandalism is believed to be 10 percent of the total losses.

Response to Losses

Librarians commonly respond to losses in a reactive, rather than a proactive manner. A common reaction to headlines about thefts elsewhere or evidence of local losses is to purchase an electronic theft detection system; the reaction to vandalism is to secure vulnerable doors and windows, and install burglar alarms and smoke detectors.

Electronic theft detection in libraries has become a growth industry with vendors selling or leasing 500 new electronic detection systems annually. The total number of installations is now over 3500. Are the collections protected by such systems truly secure from theft, or do the librarians have a false sense of security? Libraries have recently begun to install burglar alarms and smoke/fire detectors, but is there any evidence that this has deterred theft and vandalism?

While of value in controlling losses, theft detection systems can instill a false sense of security because they protect only the entrances at which they are placed. The systems stop the forgetful and the unskilled, but offer no protection against a person intent on stealing. A number of the libraries that suffered losses at the hands of Shinn and Freeman had electronic security systems in place and operational. Nor are burglar and smoke/fire alarms fully reliable, because in several of the arson incidents reported in the past three years the protective systems were not working or had been incapacitated.

It is generally recognized that any security system can be compromised. The targets or strips placed in books to trigger the theft detection alarm can be removed, the book or other library material can be wrapped in shielding material, or a powerful magnet can be used to foil the sensors. Smoke detectors cannot only be deactivated, but can be set off again and again so that they cease to be taken seriously.

These problems are beyond the control of individual librarians except insofar as they can influence vendors to improve the reliability of their products. However, there are a number of factors which affect security which are within control of the librarian. They are the subject of this article.

Defining Security Needs

Traditionally, security has been a matter of devising safeguards in reaction to specific losses. That is to say, when a loss occurs a new safeguard is introduced to protect against recurrence of that type of loss in the future. Libraries cannot afford the luxury of continuing such an approach; security must be viewed in the broadest possible sense and librarians should engage in anticipatory planning.

Library administrators should define the collection security needs broadly, encompassing in the review the security of materials from theft, fire, flood, and vandalism. Included in the definition should be protection of materials against removal from the inventory by modifying machine-readable bibliographic records. This is the area which has been most widely ignored. Librarians have apparently assumed that their computers function in benign environments. The major concerns appear to have been accidental losses of records from errors, omissions and natural disasters. The experience of the business community suggests that security planning should also encompass the protection of computer records against deliberate alteration.

A library should not limit its approach to the physical protection of assets through such means as locks, barriers and guards. Security audits of several public and academic libraries have revealed numerous architectural elements, policies and procedures that seriously limit the usefulness of the electronic security system in those libraries. These will be discussed in the next several pages.

Typical Facilities' Weaknesses

Virtually every library has some windows that open yet lack secure screens. Library materials can be dropped to the ground and picked up later. A single unsecured window can mean the loss of hundreds of items annually. On one college campus it has been general knowledge among students that the "long-term checkout windows" are in the restrooms.

Emergency exits are also a frequent weak point. Some are not equipped with alarms; many alarms are not in working order because

they are not tested at regular intervals; and most are located beyond the visual control of the staff. Staff in libraries periodically hear the alarm go off, but, when it takes several minutes to reach the door, there is nothing they can do but shrug their shoulders.

Libraries are equally vulnerable to illegal after hours entry. Ground floor windows without grills, and doors with breakable glass, removable hinge pins and without dead-bolt locks are common.

Fire and smoke detectors are often placed so low that they can be disconnected, broken or set off. Settings of smoke detectors often are not properly calibrated or maintained so that a person blowing cigarette smoke can set them off.

Computer rooms are often kept unstaffed and unlocked. The key is usually on a master available to a large number of people. Most computer rooms are equipped only with a single fire extinguisher which staff may not be trained how to use.

Policy and Procedure Weaknesses

Many of the weaknesses in a library's security are not attributed to physical conditions, but to policies and procedures which aid the culprit or which annoy patrons and staff and lead to anti-library attitudes. Among the policies and procedures that weaken a library's security are:

1. *Restrictive access conditions.* Libraries with very limited evening and weekend hours discourage frequent trips to the library and thus encourage theft. The situation may be aggravated by lack of parking and public transportation.
2. *Keys.* Keys to the library are given out freely to users and staff and no regular inventory of keyholders is maintained. The keys are frequently of the type that can be easily duplicated. Locks are seldom changed.
3. *Exit control.* There may be no exit control or the control point may be staffed for long hours by people who lack the interest and the interpersonal skills to be effective in screening patrons. Staff manning such control points are rarely given any special training for their tasks. The flow of people leaving may be unrestricted so that people can freely pass behind those being inspected.
4. *Unauthorized possession/occupancy.* Many libraries lack written policies and procedures to guide the action to be taken upon the discovery of a person in the possession of library materials which have not been properly charged out, or when an unauthorized person is found in the the building after hours. In the absence of

appropriate guidelines, employees must use their own judgment in these situations. The possibility of patron complaints, and the threat that employees may be cautioned against overzealousness as a result, leads many to play it safe rather than risk offense.

5. *Rules and statutes.* Library rules and statutes of the associated municipality, corporation or academic institution frequently fail to address penalties for the unauthorized removal of, or damage to, library materials.
6. *Property marking.* Some libraries do not stamp all edges and the title pages of library materials because of concern about aesthetics or cost. Microforms are often not marked at all.
7. *Loans and renewals.* Short loan periods and/or restrictive renewal policies may encourage unauthorized removal or retention of library materials as may the categorization of open stacks materials as noncirculating.
8. *Circulation systems.* Policies or systems which do not require a borrower to have a library or identification card to charge out library materials can encourage delinquency. Circulation control systems which use machine-, but not eye-readable transaction cards are open to abuse in that borrowers can switch cards from one item to another.
9. *Photocopying.* Invitations for abuse may be increased when photocopy machines are limited in number, poorly located, ill-maintained, or expensive.
10. *Security manual.* Every library should have a security manual setting forth what to do to maintain security and how to deal with emergencies. It should include at least the following:
    - —Each staff member's responsibilities for maintaining security and in emergencies.
    - —Appropriate phone numbers for fire, police, library administrators, etc.
    - —Location of power switches.
    - —Copies of insurance policies.
    - —Documentation for recovery after an emergency.
11. *Termination.* Security can be endangered by the lack of systematic procedures for library cards to be renewed periodically or surrendered when leaving the institution or organization. Similar problems result from a failure to recover employee identification and keys from departing employees.

Conducting a Security Audit

Electronic security systems, burglar and smoke/fire alarms do probably reduce losses, but they cannot indefinitely compensate for the lack of an overall security plan. Such a plan can be developed by auditing library facilities, policies and procedures to identify the factors that may contribute to poor security. A series of procedures can then be developed to address the weaknesses.

Before expending any funds on electronic security devices or any other security measures, a library should be subjected to a systematic security audit to determine its vulnerability. The cost of such an audit will be a small fraction of the cost of the security measures and will assure that the steps taken are responsive to local needs, not ones reported by other libraries. The elements in a security audit should include:

I. Nature of the community, campus or organization
   - A. General description
   - B. Size
   - C. Degree of isolation
   - D. Prominence of the collections
   - E. Attitudes of staff and users

II. Indicators of security weaknesses
   - A. Evidence of theft
     1. Complaints
     2. Collection count
     3. Inventory
     4. Random sampling
   - B. Evidence of vandalism, including mutilation
   - C. Patterns of past losses
   - D. Existence of valuable special collections
   - E. Vulnerability of building
   - F. Lack of key policy
   - G. Lack of written closing procedures
   - H. Lack of unauthorized possession/occupancy policy
   - I. Lack of written access policy
   - J. Inflexible loan policy
   - K. Inflexible renewal policy
   - L. Lack of written termination procedure
     1. Employees
     2. Patrons

M. Limited property marking
N. No participation in theft alerting clearinghouses

III. Observation of present security points
  A. Principal exit(s)
    1. Location(s) necessary
    2. Security system installed
      a. Full-circulating
      b. By-pass
    3. Guards
      a. Full search
      b. Random search
      c. Casual
      d. Purses checked
    4. Restricted flow
    5. Patron behavior
    6. Characteristics of doors and locks
  B. Emergency exit(s)
    1. Visual control
    2. Alarm
    3. Electronic recording
    4. Characteristics of doors and locks
  C. Employee exit(s)
    1. Visual control
    2. Staffed
    3. Locked
    4. Characteristics of doors and locks
  D. Loading dock
    1. Visual control
    2. Staffed
    3. Locked
    4. Characteristics of doors and locks
  E. Windows
    1. Locked
    2. Secured with screens
    3. Alarm
    4. Ease of breakage
  F. Utility tunnel(s)
    1. Locked
    2. Exits
  G. Ceiling type
    1. Access to security system
    2. Crawl space

H. After hours concealment
    1. Ease of concealment
    2. Ease of exit
I. Special collections
    1. Locked
    2. Alarm
    3. Characteristics of doors, windows, ceilings
    4. Ease of concealment
    5. Ease of exit
J. Exhibit cases
    1. Secure
    2. Alarm
K. After hours book return
    1. Capacity
    2. Ease of removal
    3. Ease of vandalism/arson
L. Smoke/fire detectors
    1. Adequate number
    2. Reachable
    3. Evidence of damage/inoperation or poor maintenance
    4. Ease of false alarm
M. Computer room
    1. Staffed
    2. Locked
    3. Availability of key
    4. Back-up for files kept off-site
    5. Fire detection
    6. Automatic fire extinguishing
    7. Use of passwording and other access controls
    8. Audit trails for record changes

The Cost of Security

Typically, the cost of a security program for a library with 100,000 volumes will be $5,000 to $10,000 to revise policies and procedures, change locks and install alarms, and repair other defects. This does not include the installation of an electronic security system. Larger libraries will have to spend correspondingly more. For many libraries the $5,000 figure represents only 165 volumes since the average item now costs $30 to acquire and process. The investment is, therefore, almost always justified.

Nevertheless, such expenditures should not be made without knowing the current rate of loss. What percentage of the collection is actually lost in a twelve-month period? Most library administrators do not wish to undertake inventories to determine loss rates. There are two less expensive options: (1) random sampling, and (2) a collection census or the actual counting of the number of volumes on two separate occasions. Both are described in Alice H. Bahr's *Book Theft and Library Security Systems.*[1] Libraries unable to reduce their losses after undertaking the minimum program should consider the installation of one or more electronic security systems.

Cost-Effectiveness

Libraries should not seek to remedy every possible security weakness. Cost-effectiveness should always be kept in mind. Safeguards may involve a wide range of costs—from no cost to prohibitive cost. A risk analysis can determine the potential for loss without the safeguards. What is the likelihood that there will be a loss if an action isn't taken and what is the probable extent of the loss? Since there is no rule of thumb or standard by which to determine how much should be spent for a safeguard given a specific cost risk, the "prudent person" method could be followed. The prudent-person criterion is that even if a loss is sustained, a prudent person would agree that sufficient safeguards were in place to protect against the loss. Therefore, those held accountable for the assets should be held blameless. This rule is not particularly satisfying or practical, but is symptomatic of the state of the art.

The Human Element

In implementing any security program, human costs and reliability should be kept in mind. A safeguard that requires no human operation or intervention during its operation is usually superior to a safeguard with equivalent protective capabilities that requires human involvement. For example, if access to an area can be controlled through a simple, logical, algorithmic process and few or no exceptions are necessary, then an automatic door-access mechanism could be superior to stationing a guard at the door. Manual functions are generally weakest in a safeguard. The human element must be assessed not only as it operates during the routine functioning of the safeguard, but also how it will operate when the person is distracted or negligent.

Conclusion

A library cannot eliminate losses, but it can reduce them if it undertakes an audit of its facilities, policies and procedures and if it takes such steps as are cost effective within its range of potential loss. It should expect to remain vulnerable to the skilled thief and the malicious vandal and should periodically repeat the security audit and random sampling of its collection. The library should participate in theft alerting service for rare books and should arrange with local buyers of second-hand books to alert it when materials bearing the library's property markings are offered for sale. If an automated system is used, the files should be protected against tampering and a back-up copy should be kept at a remote, secure location.

Reference

1. Bahr, Alice H. *Book Theft and Library Security Systems, 1981-82.* White Plains, N.Y.: Knowledge Industry Publications, 1981.