Electronic Security for Books

ALICE HARRISON BAHR

Overview

TWENTY YEARS AGO, electronic protection for library materials was virtually unheard of. Only one system was on the market, a metal detection system developed by E.M. Trikilis of Sentronic International, now a subdivision of General Nucleonics, Inc. Four years later, Checkpoint Systems, Inc., entered the marketplace by installing and testing another metal detection system in several branches of the Free Library of Philadelphia. The early systems were successful, but problems with false alarms and target size and adhesives led to the development of new systems in the early and middle 1970s. In 1970, 3M introduced an electromagnetic system. Three years later, Checkpoint released a radio frequency system and librarians declared the 1970s the age of electronic security.

By the end of that decade, librarians could choose among systems available from Checkpoint Systems, Inc., Gaylord Library Systems, Knogo Corporation, Sentronic International, and 3M. Other companies had developed or were considering developing systems. Innovative Systems had designed an interface between an electronic security system and an automated circulation system that let users charge out and deactivate library materials by themselves. As late as 1980, Sensormatic Electronics Corporation, the leading retail security system vendor which had tested an early library system, was considering the development of a new one. Despite that flurry of activity and interest in elec-

Alice Harrison Bahr is Project Librarian, Muhlenberg College Library, Allentown, Pennsylvania.

tronic protection of library materials, today there are only three vendors actively marketing systems to libraries: Checkpoint, Knogo and 3M. Knogo has about 300 U.S. library installations, Checkpoint approximately 2000 and 3M between 3000 and 4000.

Concerns/Issues

Today's security systems, all in at least their second or third generations, have continued to change since their inception. Yet the questions asked about them remain the same. Are they effective? Are they affordable? How do they work? Which one is best? Certainly the most pressing question is whether or not electronic security systems are effective. Most libraries installing systems report loss reductions of 60 percent to 95 percent. Unequivocally, electronic security systems work, but there are some kinds of library losses they were never designed to prevent. They will not recoup unreturned overdues, properly checked out materials that are not returned. They cannot control, and in some rare instances foment, mutilation of materials. Targets are rarely suitable for rare book, map and manuscript collections. Whether targets are 1.5 x 1.5 inch labels with adhesive peel-off backings or 6.5 x .2 inch adhesive strips, they deface valuable materials, are difficult to place on some, and in many would be highly visible.

There are additional constraints on system effectiveness. No system is foolproof, especially against premeditated thefts. If it were, reduction would be 100 percent. Not-so-clever thieves can find and remove targets. The tall can hold materials over their heads, the graceful can kick them along the floor, the athletic can toss them out windows. Open stairwells and multiple exits may frustrate security. After moving into a new facility that made exit control difficult, the C.W. Post Center of Long Island University discovered a 10 percent collection loss.[1] The relatively high level of system effectiveness becomes a compliment to the majority of library users, few of whom are premeditated thieves.

Under the circumstances in which they were designed to be effective, electronic security systems work well, and the spiralling cost of library materials contributes to their affordability. In 1977 the average per-volume price of a hardcover book was $19.22.[2] Medical hardcovers were slighly higher, $24.[3] By 1982 those prices had risen respectively to $30.59 and $38.71.[4] Even with elimination of volumes costing $81 or more, the average per volume price of a hardcover rose from $17.32 in 1977 to $23.13 in 1982.[5]

Consider a library with an annual loss of 500 materials. Presume that within a year 13 percent of the materials thought lost will reappear on the shelves. That reduces actual losses to 435. Presume further that an electronic security system will be only 80 percent effective. It will save only 348 of the 435 materials. Last, presume the library's policy is to replace all missing volumes. At a per-volume cost of $23, replacement alone would cost the library $8000.

The average cost of an electronic security system is between $10,000 and $13,000. That includes equipment, installation, service for one year, and targets to protect 20 percent of a 100,000 volume collection and 10,000 new acquisitions. A library with a single entrance and exit and with a collection of 40,000 losing 1 percent of its collection annually would pay for an electronic security system in a year. In a special library with more expensive materials, payback would be even sooner. This relatively quick payback period is shortened if losses are greater than 1 percent. In most libraries, they are. The estimate of loss in American high school libraries is between 5 percent and 10 percent per year of total collections (see table 1 for relative cost comparisons).[6]

Determining the Need

While effectiveness and affordability are basic questions, a more important one is often lost in the shuffle. Does the library *need* an electronic security system? Substantial loss alone does not warrant purchase. Need should be gauged not only by the extent but by the nature of losses that can be attributed to theft. Determining either or both requires collection study. Studies can be informal. How many materials purchased two years ago are still available? Has the annual search file grown substantially over the years? How about high-demand subject areas? Are materials either on the shelves or in circulation? How many nonprint materials are missing? These less formal means offer a rough justification for the expense of an electronic security system. But more formal studies can be designed to answer the following important questions: (1) how great is the extent of overall loss? (2) how great is the extent of annual loss? (3) how much loss can be attributed to theft rather than to unreturned overdues, legally borrowed materials that will eventually be returned, and to material mutilation? (4) how many stolen titles would the library choose to replace? and (5) what type of material or what subjects are most frequently stolen?[7]

The nature of loss requires as much study as does the operation of available systems. Answering questions about both is the quickest way

to determine which system is best. Which is best is a function of need. If most loss results from mutilation, for example, there are options other than electronic protection. Closed stacks often are preferred—and for more than one reason. American University houses journals in closed stacks not only to reduce theft and mutilation but to gauge use for collection evaluation studies. Other libraries with a high incidence of journal mutilation rely on other forms of surveillance, such as video cameras and regular stack patrols. At regular intervals, staff members walk through the library and ask patrons if they need help. To minimize theft of audiovisual materials at least one community college duplicates some audiovisual materials, and originals remain in the library in closed stacks.

The need for an electronic security system depends as well on building plans, automation plans, alterations in routine processing procedures, and staff support. And last, it entails an understanding of the different ways in which currently available systems work.

How Current Systems Work

Currently available electronic security systems operate in basically the same way. In all, special targets are placed in or on library materials. In all, patrons exit the library by walking between sensing screens, units or columns. These screens are equipped to detect the presence of targets that have not been deactivated. Active targets trigger audio/visual alarms and result in exit gates or turnstiles locking.

These systems operate in one of two modes: bypass and full-circulating. In the bypass mode, desk attendants bypass the system by passing materials behind the sensing screens to exiting patrons. The targets are never deactivated. This mode is less expensive since no equipment is required to activate or deactivate targets. It is recommended in libraries where patrons check materials out and return with them only when they are due. In a full-circulating mode, targets are activated and deactivated. This mode is recommended for libraries whose patrons return frequently with previously checked out materials.

Despite some similarities, there are a number of operational differences among systems. Most are related to the principle upon which the systems operate. Currently available library systems operate on one of two principles: electromagnetism and radio frequency. Knogo and 3M offer electromagnetic systems to libraries. For a long time, Checkpoint marketed the only radio frequency library system. In 1984, 3M introduced one called Echotag.

TABLE 1
COST COMPARISON FOR ELECTRONIC SECURITY SYSTEMS

System	*Sensing Screens (Single Aisle)*	*Charge/ Discharge Units (unit)*	*Entrance/ Exit Gates/ Turnstiles (unit)*	*Installation (Single Aisle)*	*Service (Annual)*	*Targets (unit)*	*Targets (quantity)*
Checkpoint Mark III	$4,400	Date Due Cards $40 per 1,000	$600-$900/ $800-$1,200	$350	$300	$.21 $.11 $.07	2,000-4,000 20,000-28,000 100,000
Knogo Mark VIII	4,600	$1,450	$700-$900/ $900	$400	$510	$.10 $.085 $.075	1,000-4,999 25,000-49,000 100,000-149,000
3M/1850	$6,375	$1,505	$550-$900	$408-$713	$523	$.145 $.127	2,000-7,000 16,000-15,000
3M/1350	$5,045	$1,505	$500-$900	$408-$713	$396	quoted	50,000

The operating principle determines where targets are placed, what materials are protected, the extent of downtime and false alarms, the width of aisles, the means of system compromise, and compatibility with online systems. In a radio frequency system, targets—usually two inches square—have tiny circuits in them. Sensing screens contain antennas. The deactivation process is manual. Targets must be placed where they can be shielded by deactivating date due cards or date due stickers. In electromagnetic systems, on the other hand, targets are magnetized or deactivated electronically. Strips—6.5 inches long with adhesive backings on one or both sides—are placed in spines of materials or between pages.

Electromagnetic and radio frequency systems protect different types of material in different ways. In a bypass mode, all systems protect any materials that can be targeted and carried from the library between sensing screens. In the electromagnetic systems' full-circulating mode, however, there is a danger of data loss on audio, video, and computer tapes brought in contact with activation/deactivation units. Some users report interference with watches brought in contact with these activation/deactivation units. Video terminals (CRTs) may be placed too close to units, which prevents active targets from triggering alarms. The Biomedical Library at the University of California in Los Angeles suffered minimal temporary difficulty when its circulation system CRTs were placed too close to the activation/deactivation units of its electromagnetic security system.

There is no conclusive evidence that all electromagnetic systems incur more downtime than radio frequency systems; however, the May/June 1979 *Library Technology Reports* indicates fewer false alarms in radio frequency systems—one every five days as opposed to one every three and a half hours in electromagnetic systems.[8]

Present and future procedures for charging and discharging materials have some bearing on the capability of an electronic security system to complement other procedures and systems within the library. In the full-circulation mode, the Checkpoint System and the 3M Echotag are designed to work with circulation systems using book pockets and date due cards. Most automated circulation systems eliminate the need for both. In so doing, they leave the library with the task of finding some way to let patrons know when materials are due. The library has the option of an auxillary printer to indicate due date or it can forego the added benefit of not having to open materials to check them out and continue using book pockets and date due cards.

Developments

In the future, libraries can expect systems to be more streamlined and less expensive. Increasingly, they will be designed to meet special security needs. These changes will result not only from growing vendor commitment to retail operations and to product enhancements but from changing library attitudes and altered budgets.

Twenty years ago when the first electronic security system was installed in the Grand Rapids (Michigan) Public Library, librarians were not always enthusiastic about the electronic surveillance in public service facilities. Locking gates and sounding alarms seemed offensive and out of place. So did the admission that library thefts were crimes. By the 1970s, however, articles like "Losses Demand Electronics," and "Quick! Tell Me How To Buy...Library Security Systems" were common.[9]

Libraries began hiring collection agencies to reclaim overdues. In 1972, the Los Angeles Public Library System started hiring field investigators to recover materials six weeks overdue. In one year, 7716 books worth $42,706 were returned.[10] In 1975, Virginia passed a law that did more than acknowledge library theft as a crime: it defined theft as willful concealment, exempted staff from criminal liability for detaining patrons for probable cause, and sanctioned arrests without warrants.[11] In 1983, dedicated librarians spent hours helping to prosecute notorious rare book thief James Shinn, now serving twenty years for stealing materials from college, university and seminary libraries across the country.[12]

Changing attitudes contribute in part to the new look of systems. Libraries like the Search Room of the U.S. Patent and Trademark Office in Arlington, Virginia (Checkpoint); the Northern Virginia Community College in Alexandria, Virginia (Checkpoint); the Anaheim Public Library in Euclid, California (3M); and the Southern California College in Costa Mesa (3M) are purchasing the installing systems without gates or turnstiles. The immediate benefit of doing this is economic—a savings of at least $1000. But there are other considerations as well. Aesthetics is one, effectiveness another. The metal in turnstiles can falsely alarm an electromagnetic system. Traffic flow is an additional consideration. Regulating traffic flow is more likely to be seen as a benefit to high school rather than to other types of libraries. Gates make fairly poor traffic controllers. Out of politeness, exiting patrons often hold gates open for the persons behing them. Finally, the absence of either gates or turnstiles makes an often ignored fact about library theft quite obvious:

it inconveniences every library user. With no gates or turnstiles in place, a sounding alarm requires several exiting patrons to return to the circulation desk. The absence of these devices signals yet another attitudinal change among librarians. It is a sophisticated attitude, one that admits the existence of theft, the library's role to prevent it, and the need to be flexible in doing so.

Another factor influencing new developments in library systems is retail trade. Both Checkpoint and 3M entered the security market with systems for libraries only. Checkpoint's sales are now 25 percent to libraries and 75 percent to retail establishments and 3M's retail commitment grows steadily. This commitment has led to product developments that increase a library's options. For instance, stores in malls require aisle widths greater than the 32 inches permitted by electromagnetic systems. Checkpoint can accommodate a three-to-five foot aisle. Target size determines the distance. 3M's Echotag permits three-to-four-foot protection on both sides of a single screen.

Not just the distance between screens but their placement has also been affected. In some stores, as in libraries, sensing screens or columns flank entrances and exits. In others, the screens are placed overhead and out of sight. Checkpoint has just developed an overhead and floor detection system for the retail market. It is likely that a comparable system will soon become available to libraries.

The deepening commitment of vendors to the retail market also opens up other potential operating configurations. For example, 3M makes a small deactivation-only unit for bookstores, the 930. It costs $75, about $1400 less than the cost of 3M's 950 which activates, deactivates and indicates whether or not materials are targeted. Knogo's wand sensitizer does the same thing as the 3M 930 and costs $350. The company gives away a strip identifier—a unit that indicates whether or not targets are present. These single-function units were designed for retailers and bookstore operators who need only to deactivate materials upon point of sale. Libraries using a full-circulating mode need to deactivate, reactivate and identify targeted materials. However, the presence of such small deactivation units at reduced costs holds some promise that less expensive reactivation units might also be developed.

Small libraries and small special libraries will benefit most from developments aimed at smaller retail operations. These libraries can expect more compact, streamlined, portable systems. They will also be less expensive. While 3M's electromagnetic systems require dedicated lines, its Echotag plugs in and costs about $3200.

Special consideration has already been given to the small libraries, like medical libraries, whose patrons have twenty-four hour access to collections. There is a Checkpoint System in the Veteran's Administration Center Library (Brooklyn, New York) that signals an alarm at the hospital security desk and locks library doors when someone attempts to exit with library materials during hours when the library is closed. It alerts a hospital guard to watch a monitor directed at patrons leaving the library with materials. The 3M can link security systems, cameras and photocopiers.

Larger libraries will continue to benefit from ongoing product enhancements. Already, sensing screens have become more streamlined, targets have become smaller, and detection has improved. Recently, Knogo improved its system's electronics to reduce overheating and to minimize service calls. Its Mark VIII has slightly higher sensing screens to provide a detection zone from ankle height to fifty-six inches, the area in which targets may be detected. In April, Checkpoint introduced a dual-frequency system. Until then, early Checkpoint System users could not take advantage of smaller targets like the Teeny Beeper (2 x 2 inches) and the Stikker (1.5 x 1.5 inches) because they operated in an 8.2 Mhz frequency system. Earlier systems had larger targets that operated in a 4.5 Mhz or 5.0 Mhz frequency. Checkpoint's dual-frequency transmitter board allows early customers to switch to smaller targets without retargeting previously protected materials.

Conclusion

The challenge for libraries today is not just to keep abreast of product developments and library security needs, but to anticipate changes in those needs and to encourage vendors to keep pace with them. Chester Pletzke, director of the Uniformed Services University of the Health Sciences Library (Bethesda, Maryland), is doing that. The library, which uses a Checkpoint System in a bypass mode, is currently experimenting with the use of a tractor-fed printer to produce call number labels in which Checkpoint-detectable circuits are concealed. Pletzke cautions that some adjustments are necessary. Smaller labels do not feed into the printer. The process, however, has potential for interfacing electronic security and automated cataloging. Libraries might simply request tractor-fed printers with their systems and specify that the systems have a capability of producing detectable call-number labels for processed materials.

As systems and collections change, so too will the pattern of thefts. How else can one account for one library's loss of a $3700 OCLC terminal and the Tucson, Arizona Woods Branch Public Library's loss of 54 percent of its nonprint materials.[13] On the horizon is the question of protection not only for nonprint materials, but for microforms and computer programs. The library needs to assess its collection development policies, building program plans, service and technical processing procedures, and staff resources to determine the present and future role of electronic protection for library collections.

References

1. Ungarelli, Donald L. "Exerpts—Taken From a Paper Entitled 'The Empty Shelves.'" *The Bookmark* (N.Y. State Library) 32(May-June 1973):155.

2. Grannis, Chandler B. "Title Output and Average Prices—1982 Preliminary Figures." *Publishers' Weekly* 223(11 March 1983):46.

3. Ibid.

4. Ibid.

5. Ibid., p.47.

6. "Quick! Tell Me How To Buy...Library Security Systems." *American School Board Journal* 164(Aug. 1977):43.

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

8. Knight, Nancy H. "Theft Detection Systems Revisited: An Updated Survey." *Library Technology Reports* 15(May/June 1979):221-409.

9. "Losses Demand Electronics." *Library Association Record* 80(July 1978):323; and "Quick! Tell Me How To Buy...Library Security Systems."

10. "LAPL Lowers the Boom on Book Thefts." *Library Journal* 95(1 Jan. 1970): 20.

11. "A Model Law Relating to Library and Archives Theft." *Archival Security Newsletter* (March 1977):7.

12. "Shinn Sentenced in Theft of Rare Books from Libraries." *The Morning Call,* 13 Oct. 1982, Sect. A, pp. 1-2.

13. "Nail Down Your OCLC Terminals." *Library Journal* 104(1 June 1979):1207; and "Security in Libraries." *Library Journal* 104(15 April 1979):878.

Top 100 Hacking & Security E-Books (Free Download). 2.7k stars. 577 forks. Star. Watch. Code. Issues 9.Â Topics. hacking books security penetration-testing ebooks kali-linux hacking-security-ebooks. Resources. Readme. Releases. No releases published. I asked several top security researchers which books helped them on their path. I also asked which books theyâ€™d recommend to people who want to follow in their footsteps. These are the titles they told me you should put on your Kindle or bedside table. Nuts and bolts.Â Eva Galperin, director of cybersecurity at the Electronic Frontier Foundation, recommends "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software" by Michael Sikorski and Andrew Honig. This book teaches readers how to safely analyze, debug, and disassemble malware, and it offers hands-on labs to help readers practice their skills. Galperin further recommends "Threat Modeling: Designing for Security" by Adam Shostack. 5,254 security for books products are offered for sale by suppliers on Alibaba.com, of which safes accounts for 4%, cctv camera accounts for 1%, and lock cylinder accounts for 1%. A wide variety of security for books options are available to you, such as cmos, ccd. You can also choose from carton sealing, tools security for books, as well as from waterproof / weatherproof, vandal-proof, and night vision security for books, and whether security for books is waterproof, or security.Â book secur suppliers cd label system suppliers china anti-theft strips china security stickers for books electronic security systems book security label magnetic book label detector em library system gateway em system jewellery eas philips battery shaver shade 1. Why Reading Information Security Books is Crucial. When it comes to learning, we have possibilities like YouTube, learning platforms, scholarly articles on Google, online courses, etc. Throughout all the years' books still somehow managed to stay the most relevant way of learning.Â Cyber security for Seniors is among the protecting cyber security books because it contains possible risks, solutions, and practices for seniors to operate on the internet. The author introduces the reader with the terminology and special web links that allow surfing the internet further. It is important to understand the possible risks that may occur in the on seniors' laptop or smartphone, how to surf the web safely, how to protect your social media and email accounts.