Chapter 10

Information Security for Libraries

Gregory B. Newby
University of North Carolina at Chapel Hill, USA

Libraries have made significant investments in computer-based resources, training and services. However, such investments need to be protected from misuse or mistake by taking an active role in information security.

INTRODUCTION

By most accounts, the proliferation of the Internet and other computer technologies has been highly beneficial to libraries. Investment in everything from online databases and computing equipment to personnel and training is significant. Libraries need to have policies, protection measures and trained staff in place in order to safeguard their investments in computer and computer-related technologies, personnel and services.

This chapter will address the topic of information security, making concrete recommendations for safeguarding information and information access tools. Instead of giving detailed instructions for security techniques, the emphasis here is on setting the agenda for the role of security in library environments.

Historically, formal training for librarians’ use of information technology was in the relatively narrow specializations of library automation and online searching. Library automation training (e.g., Ross, 1984) was for library staff that would manage, evaluate, and sometimes design and implement technology systems in libraries. The OPAC (Online Public Access Catalog) was a centralized system based in the library or a regional office for circulation and holdings information, as well as other types of data (serials control, acquisitions, cataloging, etc.). Library automation training seldom mentioned any type of security for protection of data.
privacy or equipment. Even fairly recent books on the use of computers in libraries, such as Ogg (1997), make almost no mention of security issues.

Today, library environments are increasingly reliant on computer technology. Many libraries of all sizes have discontinued use of card catalogs in favor of electronic versions – and many of the electronic versions previously accessible only via terminals within library buildings are now Web-accessible. Online searching of a plethora of databases and other information sources has become ubiquitous for the end user, rather than being restricted to librarians trained in online searching. Access to general-purpose microcomputers and software, as well as to the Internet, is offered in nearly all libraries of significant size.

It is the position of this chapter that security training for librarians is extremely weak, both on the job and in educational institutions. One result is that opportunities for problems related to information security in libraries are likely in many library environments. Although some recent texts on library security address aspects of information and computer security (for example, Shuman, 1999), most do not.

In this chapter, a pragmatic approach to addressing the information security needs of libraries is presented. Effective information security must involve active staff and active measures to minimize risk of damage, theft, subversion or sabotage. Following an overview of information security, sections discuss security personnel, privacy policy, the OPAC, public access workstations, and the library’s Internet connection. A concluding section addresses the emerging role of security training for librarians.

OVERVIEW OF INFORMATION SECURITY

Information security is not simply computer security. Whereas computer security relates to securing computing systems against unwanted access and use, information security also includes issues such as information management, information privacy and data integrity. For example, information security in a library would include personnel security and policies, steps taken for effective backups, and the physical integrity of computing facilities.

According to a recent survey of executive recruiters, computer security experts are among the six most sought-after professionals for the corporate world (Radcliff, 1999). Yet, there are very few college courses addressing computer security. Those that do mostly emphasize the mathematics of encryption rather than hands-on information security and management.

Minimally, effective information security in libraries should include:

• Staff assigned to information security tasks
• Training all personnel in information security issues and procedures
• Specific policies dealing with information privacy, physical security of equipment, and computer security procedures
The NGO Forum
www.igi-global.com/chapter/ngo-forum/17729?camid=4v1a