Bibliographic Essay Unit 3
Gregory Tharp, Marissa Antosh
September 11, 2008

Hardware Issues

Introduction

Prior to the turn of the century libraries were typically considered to be institutions where librarians helped individuals locate tangible items (i.e. books) by using a card catalogue. Now libraries are thought of as institutions where librarians help patrons to find an appropriate tangible or intangible item (i.e. a website) based on the individual's needs. But as technology developed, so did the needs of library users. According to Siewiorek et al. (2004), the large mainframes of the 1970s which required approximately 5,000 hours of training and a BS in engineering to operate have given rise personal computers and mobile devices (e.g. cellphones) which only require training at the time of purchase to operate (p. 110). This trend gave libraries the opportunity to shift away from the typical model where librarians help individuals locate tangible items (i.e books) by using a card catalogue towards a model where librarians help patrons to find an appropriate tangible or intangible item (i.e. a website) based on the individual's needs. Even though it appears that libraries can easily train its patrons and staff on emerging technologies (i.e. personal computers) in a matter of hours, they were still faced with dealing with "hardware as an error source" (Siewiorek et al., 2004, p. 110). This meant that no matter if libraries used the latest personal computer or a personal computer from the 1980s for their operations, libraries were still faced with the prospect that they invariably have to contend with architectural and other issues arising from the use of hardware.

I: Architectural/Infrastructure Issues

Libraries are faced with a variety of architectural issues in utilizing hardware, which chiefly include maintaining security of its computer infrastructure as well as applying cutting edge hardware to its operations. Security concerns for libraries include "hardware, CMOS (Complementary Metal Oxide Semiconductor), boot" (Ives, 1996, p. 40). Since the system unit (or CPU case) and any peripheral devices (e.g. printers) makes it easy for the library user to input data (e.g. by typing on the keyboard) and output the data (e.g. by printing a document), libraries must ensure that the system unit and peripheral devices remain in working order in order to entice library users to return to the library repeatedly. The library can guard against intentional (e.g. theft) or unintentional (e.g. being jostled from proper position) acts that may render the system unit and or peripheral devices inoperable by undertaking the following security measures. Libraries should ensure that "all network wiring closets should be kept locked and accessible only with a nonstandard key or combination lock, the CPU case should be locked with its OEM (Original Equipment Manufacturer)-provided lock and should also be connected to peripheral devices wires running through a keylocked steel box" (Ives, 1996, p. 38). By physically locking the system unit and wiring for peripheral devices, libraries are reducing the chance that library users intentionally or unintentionally render the system unit inoperable which helps to ensure that library users have an enjoyable experience using the library's computers.

Aside from having to adapt security measures to prevent physical acts against the system unit and peripheral devices, libraries are also faced with the challenge of protecting the operations of the chips on its computers. In order to protect its CMOS, chips which control the actions of each computer's CPU (Central Processing Unit (Williams et al., p. 208)) and boot process, libraries should "password both the computer's CPU setup menu and CPU-boot system with character strings not found in any dictionary as well as have the computer boot from hard disk only" (Ives, 1996, p. 38) By putting a strong password on both the CPU setup and CPU boot, libraries are preventing library users from unintentionally (i.e. by striking a wrong key during the boot process) or intentionally (i.e. by launching a virus) altering how the library computers boot. By taking this measure, libraries are ensuring that library users have a pleasant experience on library computers and thus return to the library.

Aside from implementing security measures on its computers, libraries must stay abreast of cutting edge technology in order to enhance library user experiences. In order to stay abreast of cutting edge technology, librarians should "read current library, management, ethnographic, sociological, and IT literature; become a lobbyist; and think 3 to 5 years out" (Huwe, 2005, p. 32) To effectively run a library, a librarian has to not only be familiar with the newest technology but also has to attempt to figure out if the newest technology is the best fit for their library. In order to make this determination, librarians must examine current trends in management and sociology in order to infer how the new technology will impact both the library user's perception and how other stakeholders (e.g. employees) perceive of their library. Aside from ensuring that cutting edge technology does not alienate their communities, librarians must also realize that sometimes entities (e.g. the board of trustees) may be slow to allocate enough resources (e.g. manpower) necessary to implement cutting edge technology and thus librarians must be their own advocate if they truly believe that a specific technology will improve library operations. Libraries must realize that once they implement a new technology, they must constantly look out for the next new technology otherwise library patrons will not feel that the library is efficiently satisfying their need for information.

Besides staying abreast of cutting edge technology, libraries must also think of practical ways to implement the cutting edge technology because after all having knowledge about cutting edge technology is useless if one does not take steps to implement it. According to the Systems Librarian journal, advances in hardware have allowed libraries to allow users to self-check out by positioning their books and library cards under a reader connected to a computer which checks the books out of the library as well as having the capability of implementing an RFID chip into materials which allows the computer to automatically check a book back into the library (Breeding, 2008, p. 20-21). Utilizing computers to both check in and checkout materials (e.g. books) from the library frees up librarians to perform other tasks (i.e. help library users locate materials) which makes libraries more efficient in serving the needs of library users. But the increasing reliance on technology to check books in and out of the library exposures the library to the risk that if any hardware (e.g. RFID chips) malfunction or breakdown, library users will have no way to check books in and out of the library without pulling librarians away from other tasks which in turn makes the library just less efficient.

Finally, the physical space of the library must be considered. Hardware is not useful if it has no place to go, so new furniture for hardware-laden areas (i.e. the circulation desk, public computers, and the reference desk) may be required (Barreau, 2001, p. 209)

II. Training/Personnel Issues

An additional issue libraries face with regard to hardware is proper training for their employees. Indeed, de Vries and Fleck (1997) were accurate when they said, "Of all the elements required to build a working client/server system, the most important and often least understood or appreciated component is people" (p. 229). Computers do not staff libraries, people do. And unlike computers, people's motivations and experiences can vary widely.

In a UK survey regarding IT and personnel management education, it was apparent that there was a "[…] reluctance by staff to get involved in these development programmes because relatively little incentive was provided by the institutions for the acquisition of IT competences" (Kinnie and Arthurs, 1994, p. 15). While it is pleasant to think that library employees would want to learn about new hardware in order to better the library's services, that is not often the case. If the hardware is changing at a rapid rate, library staff may feel bogged down by the continual training requirements. Also, staff bring a wide range of computer experience with them: "At one extreme, there were students who did not know how to turn the machine on. At the other extreme, there were students […] who were familiar with highly sophisticated applications of IT in personnel and were saying, "What can you teach us?"" (Kinnie and Arthurs, 1994, p. 16). It is near impossible to standardize a training program for new hardware when not every employee is starting from the same point.

Cost is another obstacle to think about when considering training employees to use new hardware. Not only is a cost incurred by purchasing new hardware, but it takes the dual resources of time and money in order to get staff ready to work with the new hardware and, furthermore, be able to instruct patrons in its use. Tebbets (2000) asserted, "Training is essential, and librarians must plan on providing on going support for staff and users in learning and using new software and hardware. Funds for this must be incorporated into the budget" (p. 132). However, funding is often inadequate, especially when budgets are tight. Furthermore, training may need to be customized to a particular organization and training must be ongoing due to hardware and staffing changes, both which must be funded as time goes on (Barreau, 2001, p. 209). The cost of hardware maintenance must be factored in as well: "[…] staff dedicated to maintaining the hardware and software as well as managing the intricacies of the network are essential to the smooth operation of the system" (Tebbets, 2000, p. 132). Whether the maintenance is done in-house or remotely, it requires a professional staff which, in turn, drives up costs for the library.

Conclusion

Libraries have to consider the full scope of hardware issues before they consider upgrading their systems. Security is of primary importance so hardware remains in good working order and patrons will continue to use the library. It is necessary for the wiring for the CPU and all peripherals to remain locked so hardware is neither intentionally or unintentionally altered, rendering the hardware useless. Libraries must also stay current with new hardware and select it for practical use. If the hardware has no practical application in a specific setting, then it reduces the library's efficiency. The physical space the hardware will occupy is another consideration. New furniture or a new configuration may need to be explored.

Finally, hardware does not exist in a vacuum, which is why it is important for training and staffing to be examined as hardware issues. Current staff may not be experienced with the new technology or may be reluctant to learn.

Tying all of these hardware issues together is the cost in both time and money to the library. Hardware alone is expensive, but when bundled with proper security, continual maintenance, and training staff, the cost escalates quickly. When choosing hardware, libraries must look at the overall picture and weigh the benefits with the issues.

References

Barreau, Deborah. (2001). The Hidden Costs of Implementing and Maintaining Information Systems. *The Bottom Line: Managing Library Finances, 14,* 207-213. Retrieved September 8, 2008, from http://0-www.emeraldinsight.com.csulib.ctstateu.edu:80/Insight/viewPDF.jsp?Filename=html/Output/Published/EmeraldFullTextArticle/Pdf/1700140402.pdf

Breeding, Marshall. (2008). Circulation Technologies from the Past to Future. *The Systems Librarian*, 19-21.

de Vries, Weitze A., & Fleck, Robert A. (1997). Client/server Infrastructure: A Case Study in Planning and Conversion. *Industrial Management & Data Systems, 97,* 222-232. Retrieved September 8, 2008, from http://0-www.emeraldinsight.com.csulib.ctstateu.edu:80/Insight/viewPDF.jsp?Filename=html/Output/Published/EmeraldFullTextArticle/Pdf/0290970603.pdf

Huwe, Terrence K. (2005). New Technology's Surprising Security Threats. *Computers in Libraries*, 30-32.

Ives, David J. (1996). Security Management Strategies for Protecting Your Library's Network. *Computers In Libraries*, 36-42.

Kinnie, N.J., & Arthurs, A.J. (1994). IT and Personnel Management Education: Evidence from a UK Survey. *Education + Training, 36,* 13-18. Retrieved September 8, 2008, from http://0-www.emeraldinsight.com.csulib.ctstateu.edu:80/Insight/viewPDF.jsp?Filename=html/Output/Published/EmeraldFullTextArticle/Pdf/0040360103.pdf

Siewiorek, Daniel P., & Chillarege, Ram, & Kalbarczyk, Zbigniew T. (2004). Reflections on Industry Trends and Experimental Research in Dependability. *IEEE Transactions on Dependable and Secure Computing, 1,* 109-127. Retrieved September 2, 2008, from http://0-csdl2.computer.org.csulib.ctstateu.edu/comp/proceedings/mse/2007/2849/00/28490067.pdf

Tebbets, Diane R. (2000). The Costs of Information Technology and the Electronic Library. *The Electronic Library, 18,* 127-136. Retrieved September 8, 2008, from http://0-www.emeraldinsight.com.csulib.ctstateu.edu:80/Insight/viewContentItem.do;jsessionid=B324D56DDF616ED6AF2CC61A7C310BEB?contentType=Article&contentId=861893

Williams, Brian K., & Sawyer, Stacey C. (2007). Using Information Technology: a practical introduction to computers & communications (7th ed.). New York: McGraw-Hill Irwin.