*IST-Africa 2015 Conference Proceedings*
*Paul Cunningham and Miriam Cunningham (Eds)*
*IIMC International Information Management Corporation, 2015*
*ISBN: 978-1-905824-51-9*

# Physical Security Measures for Computer-Based Information Systems: a Case Study of Selected Academic Libraries in Kenya

Rose W. NJOROGE[1], Daniel M. WAMBIRI[2], Nobert OGETA[3],
*Kenyatta University, P.O. Box 43844, 00100, Nairobi, Kenya*
[1]*Tel: +254 20 8710901-19, Fax: +254 020 8711575, Email: njoroge.rose@ku.ac.ke*
[2] *Tel: +254 20 8710901-19, Fax: +254 020 8711575, Email: wambiri.daniel@ku.ac.ke*
[3] *Tel: +254 20 8710901-19, Fax: +254 020 8711575, Email: Ogeta.Nobert@ku.ac.ke*

**Abstract:** Information and Communication Technology (ICT) is increasingly becoming an important facilitator of effective and efficient delivery of services in higher education institutions (HEIs). The introduction of open, distance and e-learning (ODEL) mode of study has made it necessary for academic libraries to incorporate computer-based information systems (CBIS) in order to facilitate easier access to information for learning, teaching and research to all library users. To meet this objective, HEIs need to put in place measures of securing these systems. This study investigated the security measures employed by selected academic libraries in Kenya. The specific objective of this paper is to address the physical measures used by academic libraries to secure their CBIS. Data was collected through observation and interviews and was analyzed, interpreted and presented using qualitative methods. Results revealed the libraries studied had taken several physical measures to protect their CBIS. Suggestions for further research are discussed.

**Keywords:** Library Computer-Based Information Systems, Physical security Measures, Disaster Management, Academic Libraries, Digital Library Systems, IT Security

## 1. Introduction

University libraries have increasingly continued to automate in a bid to effectively and efficiently meet the information needs of their students, lecturers and researchers. A library, being the heart of any learning institution, is strategic in meeting its clients' learning, teaching and research objectives. With the introduction of open, distance and e-learning (ODeL), part-time programmes, as well as incorporation of digital collections in libraries, it is paramount to facilitate increased access to information. Computer-based library systems that support increased access must therefore be safeguarded to ensure that they are functional, efficient and effective at all times. Disaster recovery planning and business continuity planning are two of the most critical components of the digital library system infrastructure, yet they are aspects that are often overlooked [1]. The neglect of computer-based information systems security is unfortunate because the consequences of being unprepared for disaster are significant. Literature indicates that two out of five organizations that experience disaster are out of business within five years [1].

Preliminary results showed that many libraries had embraced ICTs for automating traditional library information systems and operations. The introduction of CBIS calls for enhanced security to ensure that information in the library is available, its integrity and confidentiality is protected. Generally, studies on disaster management in libraries have concentrated on security issues affecting printed information resources and library buildings as well as methods of preventing security breaches in a traditional library [2] [3] [4] [5].

Threats to CBIS and methods of ensuring security for CBIS are quite different from those in a traditional library. There is a gap in literature of the methods used by libraries in Kenya to ensure CBIS are protected. Security of library CBIS is paramount to ensure high availability of library services and operations, and also protection of the huge investments in these systems. In particular, physical security is key to all other Information Technology (IT) security measures, yet organizations normally neglect it [6]. It is in this light that this study focused on physical measure the libraries in Kenya have put in place to protect the CBIS as a way of ensuring that libraries continuously meet the information needs of their users.

## 2. Objectives

The study aimed to investigate physical measures employed by academic libraries in Kenya to secure their library computer-based information system.

## 3. Research Methodology

The researchers used the following research methodology.

### *3.1 Research Design*

Exploratory research design was used in this study because there was need to understand the physical measures employed to secure CBIS in university libraries in Kenya since not much has been documented on this issue. The approach was preferred because the topic was relatively new and had not been explored or addressed with the sample or group of people involved in this research. There are several characteristics of an exploratory research design [7]:

> the concept is "immature" due to a conspicuous lack of theory and previous research; a notion that the available theory may be inaccurate, inappropriate, incorrect, or biased; a need exists to explore and describe phenomena and to develop theory and the nature of the phenomenon may not be suited to quantitative measures.

Data collected did not allow quantitative analysis and exploratory design was therefore appropriate for this study. In qualitative research design approach, a researcher gathers multiple forms of data through interviews, observations, documents, rather than rely on single data source [7] [8]. Data was therefore collected using observations, interviewing, audio-recording and photographing.

### *3.2 Sample and Sampling Procedures*

Target population included libraries from private chartered and public universities within Nairobi County and the neighboring counties. For the purpose of the study two (2) Chartered Private and two (2) Public Universities were selected for the study. Respondents were purposely selected from the four universities since those with relevant information were known. These included four (4) ICT directors, four (4) University Librarians, four (4) Information systems Librarians and four (4) ICT technicians.

### *3.3 Data Collection Instruments and Administration*

Data was collected using various methods which included interviews and observations. The researchers personally interviewed the respondents, visited the libraries and made observation on observable measures used to secure CBIS and took photographs of the observable measures.

### *3.4 Data analysis and interpretation*

Data was analyzed qualitatively using narratives, direct quotations from the respondents and plates for illustrations. To protect identity of the libraries studied, codes were used to represent the libraries studied as follows: L1, L2, L3 and L4 where L represents library.

## 4. Results

The research findings revealed that academic libraries in Kenya had taken several physical measures to secure their CBIS.

### *4.1 Physical Measures*

Physical measures that the libraries had put in place and were observable and identified during the study included the following:

#### *4.1.1 Use of Steel Wire*

To curb vandalism, L1 had chained the cables together using steel wire. This was meant to prevent computers from being opened as well as prevent computer peripherals such as mice and keyboard from being stolen. In addition, L1 was big in size and it was a challenge to place security guards in all areas where computers were located. This was confirmed through observation as shown in Plate 1 and Plate 2 below. This was done due to the fact that vandalism and theft of computer parts had been identified as threats to CBIS.

Hardened wire used to tie CPU cabinet at the back

*Plate 1: Hardened Wire Used to Tie the CPU Cabinet at the Back in L1. Source: Observation.*

Hardened wire used to tie the cables together

*Plate 2: Hardened Wire Used to Tie Cables Together in L1. Source: Observation.*

#### *4.1.2 Use of ”Tiebacks”*

Use of ”tiebacks” also referred to as clips, where cables were tied tightly at the back. This was observed in L2, L3 and L4. This was used to discourage or prevent theft of power cables, network cables, keyboards and mice. This was observed as illustrated in Plate 3, Plate 4 and Plate 5.

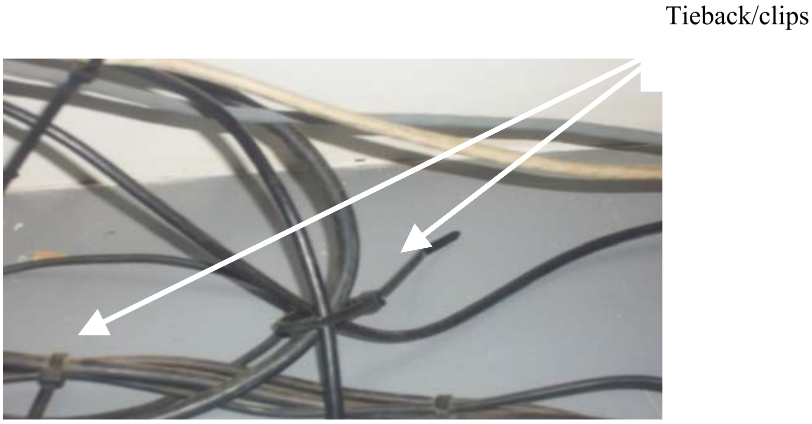

*Plate 3: Tie Back/Clip Used to Tie Cables Together in L2. Source: Observation.*

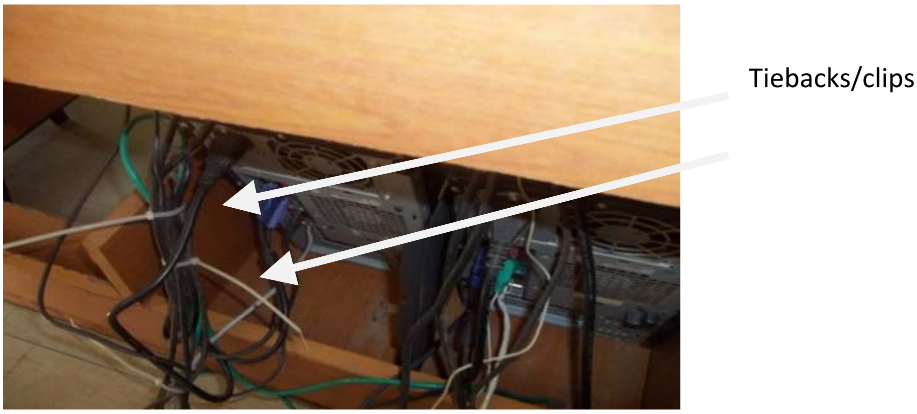

*Plate 4: Tiebacks/Clips Used to Tie Cables Together in L3. Source: Observation.*

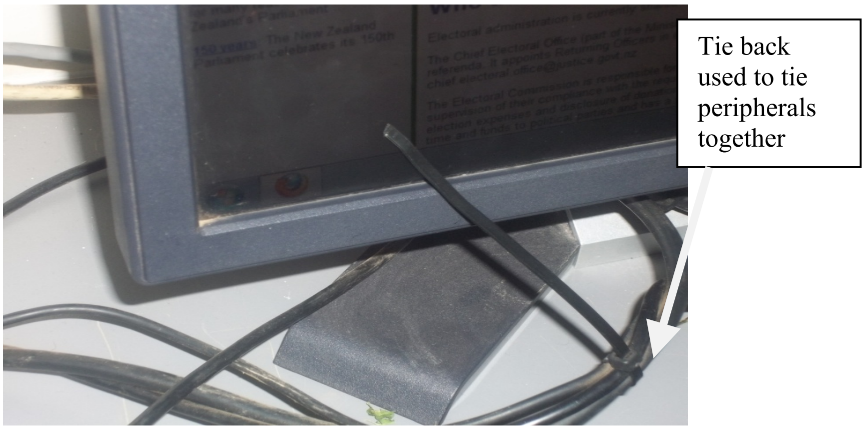

*Plate 5: Tiebacks/Clips Used to Tie Peripherals Together in L4. Source: Observation.*

### *4.1.3 Use of Lock and Key (Padlock)*

Use of lock and key (padlock) to lock the CPU cabinet to prevent anyone from removing parts of the computer or tampering with the inside of the computer. This was as shown in Plate 6 below as observed by researchers in L4.

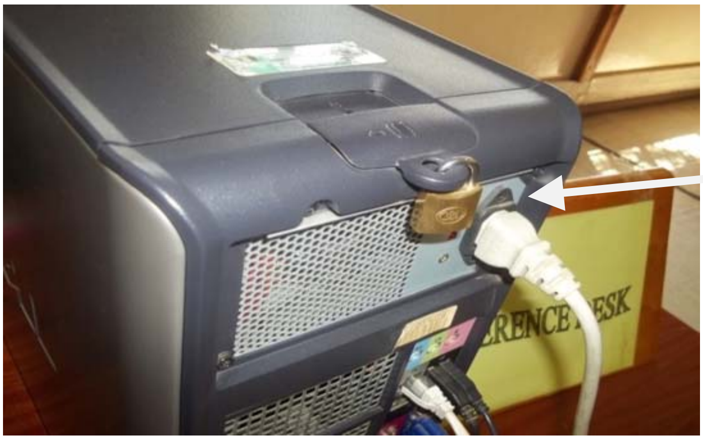

*Plate 6: A Padlock was Used to Lock the CPU Cabinet in L4. Source: Observation.*

Lock and key were also used by all libraries curb theft of computing equipment in offices, the server rooms, cabinets and computer labs in the libraries. In addition to the use of lock and key, only L1 indicated use of control measures such as record keeping and centralized place for storing keys as a measure to enhance security of CBIS. In L1, ICT Technician had this to say on security of hardware:

> On the level of hardware we ask people to be cautious of their environments…keep them under physical lock and key that at least ensures you have solved the loss of hardware, locking of offices, locking of our cabinets where equipments are stored.

Although use of lock and key to secure CPU cabinet was noted in only L4, this was a measure that L1 was contemplating taking except that it took too long to deliver padlocks and, therefore, the library had to improvise by using hardened wire to tie the CPUs cabinets, peripherals and cables together as shown in Plate 1 and Plate 2.

### *4.1.4 Tagging (Engraving Codes)*

Tagging (engraving codes) on the equipment was another method used to deter would be vandals or thieves. Marking or tagging the peripheral equipment that were targeted for theft or vandalism had been used in areas that were easy to identify or see to discourage theft of the peripheral equipment such as mice, keyboard, UPS among others. Plate 7 illustrates this which was captured through observation in L1.

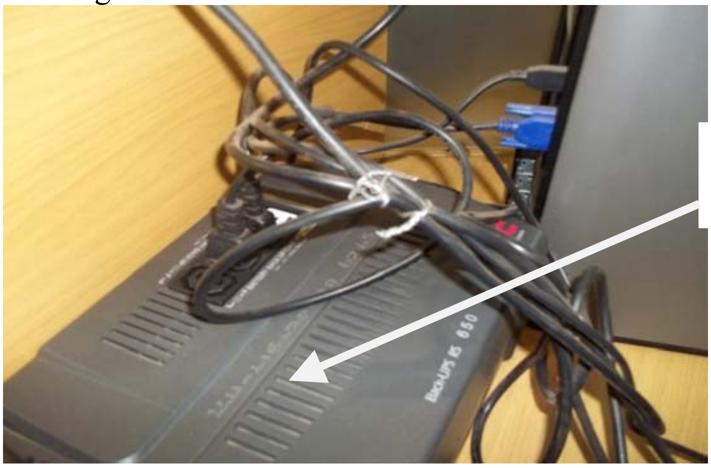

*Plate 7: Engraved Codes on the UPS in L1. Source: Observation.*

### *4.1.5 Use of Magnetic Strips*

L1 used tagging (engraving codes) as well as putting magnetic strips in some "hidden" parts of the equipment to ensure any equipment leaving the library was detected by the electronic security system at the exit door. The magnetic strips were not observed by the researchers as the respondent felt it was a breach of security and confidentiality to seek such information. Allowing the researchers to observe areas where the magnetic strips had been put was seen as a threat to security itself.

### *4.1.6 Use of Closed-Circuit Televisions (CCTVs)*

L1 used CCTVs to monitor the happenings at the Online Public Access Catalogue (OPAC) areas to prevent vandalism of computers. They were installed in the essential areas where theft had been reported to have taken place. This was done at each floor where the computers were located especially the OPAC computers which were highly targeted for vandalism, theft, and unauthorized downloading of software. Information Systems Librarian (ISL) from L1 noted that:

> On each floor we have 18 computers for OPAC, these are the ones mainly targeted for vandalism and we have therefore put in place surveillance cameras to monitor the happening in these areas.

Although the surveillance cameras had been put in place as a measure to monitor the happenings and probably catch those who vandalized the computers, it was noted that the surveillance control room where monitoring was meant to occur was in most of the times left without anyone to check what was happening in these areas. It was also noted that the L1 had not put any warning to the users that the library is under surveillance cameras. This knowledge would otherwise deter would be vandals.

### *4.1.7 Personnel*

Securing CBIS using personnel was done at two levels:

a) *Use of the Library Staff*

Library staff was used to man various places where computers used for research purposes were concentrated. Other personnel manned computer labs in the library. They played a double role as reference persons in the library as well as in surveillance in order to deter vandalism in these areas. Library staff had also been sensitized to ensure they are vigilant on the happenings within the library as well as ensuring they protected their passwords. ISLs and ICT Technicians (ICTT) from L1, L3 and L4 of the target libraries mentioned that they held staff responsible for computers in the library as well as for the ones they used in their offices. This was done to ensure protection of the hardware, applications, and data within these computers. Commenting about the high level of vandalism in L1, ISL from this library mentioned that they had:

> Alerted people at each floor and we told them if anything is removed they will be responsible. The security guards, cleaners, librarians, everybody was told to be vigilant. …there is a system where everybody is made accountable of what is lost whether a guard or a library staff.

This seemed to have worked because L1 and L3 reported to have charged security companies for computers that had been stolen from them. Security guards were charged because a monitor was stolen from the L1 and a computer from L3 and the library staff felt that a monitor or a computer are big enough to have been noticed at the exit door which the guards manned. Staff manning the computer laboratories ensured that users did not install software into the library computers. They also ensured that theft and vandalism did not take place in the computer laboratories.

Through observation, it was noted that the majority of the staff manning computer laboratories in all the libraries, did not do much to check what the users did. They were located at a corner and the only thing they were concerned with most of the times was clocking in of the users, although the users did this voluntarily. Laboratory assistants in L1 were observed to be on Facebook or listening to music most of the times and did not go round checking what the users did.

b) *Security Guards*

Two of the libraries (L1and L4), had security guards who were employees of the institutions but not trained librarians. In other two libraries (L2 and L3), guards from security companies were used. In all four libraries, the guards were used to man the exit door and to check what each person leaving the library was carrying. The guards also made rounds in the library to check any person who could be vandalizing computers. This was used as a way of deterring users from vandalizing computers or even stealing them. An ICTT from L1 had this to say:

> We have been seeing our security guards walk around the floors especially during the day when the traffic is high. They always go checking whether someone is doing something funny or something that one is not supposed to be doing.

Security guards were also given the task of ensuring security around the building especially at night as a way of preventing thieves from breaking into the building or even users stealing and passing computing equipment from the library through the windows. [9] concur with this as they note that preventive controls are those which mitigate or stop a person from acting criminally or which prevent an event from occurring such as use of password, guard and security lock.

### *4.1.8 Security Lights*

In L1, good security lighting at night outside the library building was mentioned as a method that the library used to deter theft from the library.

## 5. Discussion

Libraries have continued to incorporate CBIS for their day to day activities with an aim of increasing efficiency and effectiveness in service delivery. This has in effect introduced vulnerabilities that were not common in a traditional library. Chief among other vulnerabilities are theft and vandalism of CBIS and especially the hardware component [9]. Vandalism and theft has been reported to be a major threat to computer systems in almost all organizations that have incorporated CBIS for their day to day activities [9] [10] [11]. Libraries have devised several methods to curb or reduce these problems as these may lead to a compromise of the basic tenets of an information system: integrity, confidentiality and availability.

The study investigated physical security measures that libraries in Kenya had put in place. The findings revealed that several measures which included use of steel wire, tie backs and tagging/coding to prevent theft of peripheral devices. This concurs with other findings where theft of computer parts compromised security of CBIS and hampered smooth learning of the business activities [9]. In some cases, padlocks were used to lock the CPU cabinet to prevent vandalism of internal parts of the computer system. This method was also used to secure rooms where critical computing equipment such as servers and backups were kept. Putting magnetic strips to hidden parts of a computer parts to curb theft was a method used by one library and this seem not to have been reported elsewhere in literature. Use of CCTV has become a common method in most libraries to prevent theft and vandalism [12], although this method seemed to be uncommon among libraries in Kenya where only one library had installed CCTV in crucial areas where computer had be put. Personnel was used to prevent unauthorized access and monitoring entry to computer rooms as this was seen as a threat to theft and vandalism [9] [10] [11].

## 6. Research Contribution

Little empirical research exists on measures put in place by libraries in Kenya to curb theft and vandalism of CBIS. This research provides a baseline on physical measures put in place on which further research could be build and explore other methods that could be used and are not covered in this research. The findings are hoped to provide an insight to the stakeholders on the seriousness the threat of theft and vandalism poses to the library CBIS and therefore exchange ideas on how best to deal with these threats.

## Conclusion

In conclusion, CBIS are vulnerable to various threats such as theft and vandalism. However, for libraries to continue offering efficient and effective services and ensuring integrity, availability and confidentiality are not compromised, methods to curb theft and vandalism needed to be addressed. Although the libraries used several physical measures, more advance and modern methods such as biometrics, software and wireless peripheral devices that users need to borrow officially or coded need to be incorporated in ensuring security of physic components of CBIS.

Further research is recommended on logical and procedural measures that the libraries have put in place given that there are other threats to CBIS such as attacks by virus, illegal downloading of illegal software, deletion and distortion of library databases among others [13].

## References

[1] H. F. Cervone, "Disaster recovery and continuity planning for digital library systems," OCLC systems & services: Internation digital library persperctivs, vol. 22, no. no.3, pp. 173-178, 2006.

[2] T. Kaur, "Disaster planning in University ibraries in India: a neglected area," New Library World, vol. 110, no. no. 3/4, pp. 175-187, 2009.

[3] Aziagola, "Disaster_control planing for academic libraries in West Africa," The Journal of Academic Librarianship, vol. 34, no. no.3, pp. 265-268, 2008.

[4] D. Wambiri, Disasterplanning and preparedness in University Libraries in Kenya, Nairobi : Not Published, PhD Thesis, 2008

[5] K. M. Kimani, "Disaster management (prevention). How well are Kenyan Information Managers Prepared?," in SCESCAL, Nairobi, 1998.

[6] F. Guil, "Computer Rooms – Meet the physical security measures" Global Information Assurance Certification Paper,April 2003

[7] J. W. Creswell, Research Design: qualitative, quantatittive and mixed methods approaches, Los Angeles: Sage Publications, 2009.

[8] L. R. Gay and G. E. &. A. P. Mills, Educational Research: Competencies for analysis and applications, London: Pearson Education, 2009.

[9] "Safeguards against Hardware theft and Vandalism:" https://securitylockdownblog.wordpress.com/2014/09/17/safeguards-against-hardware-theft-and-vandalism/ accessed 31st March 2015.

[10] "INSPECTION REPORT: Security Vulnerabilities – Protecting Information and Property in the GSA Central Office Open Space"Report Number: JE15-001October 16, 2014

[11] Physical Security Continues to Dominate HITECH Breaches http://www.precyse.com/precysesource/newsletter/issue14/articles/securitycorner.php. Accessed 31st March 2015

[12] R.C. McClung, P. h; Roberts, "Method and apparatus for controlled access to a computer system" . Aug 21, 1990.

[13] J. Carney, " Why Integrate Physicaland Logical Security?" (http://fedtechmagazine.com/article.asp?item_id=512) Accessed 31st March 2015.