International Journal of Library and Information Studies
Vol.9(2) Apr-Jun, 2019 ISSN: 2231-4911

Access and Security Dilemma: A Focus on Information Security Challenges in Masvingo City Center Public Libraries, Zimbabwe

Mthokozisi Masumbika Ncube
Lecturer
Department of Information Science and Records Management
Zimbabwe Open University Midlands Regional Campus
No.16 Victory Road, Gweru
e-mail: ncubem@zou.ac.zw / ncubem.masumbika@gmail.com

Abstract - *Information Communication Technologies (ICTs) have provided extensive advantages to public libraries in ensuring access to a wide array of informational resources. However, the use of such ICTs has also brought about information security challenges within public libraries. Therefore, the premise of this study was to assess the information security challenges faced by Masvingo City Center Public Libraries. The study was qualitative in nature, using libraries' staff members, libraries' committee members, Zimbabwe Library Association Masvingo (ZIMLA) representatives and libraries' patrons as study participants. The study found that the libraries lacked rigorous antiviral software to protect computer resources. In addition, there was the Bring Your Own Device facility (BYOD) which further compromised the confidentiality of internal information within the libraries. The study concluded by highlighting that the libraries were vulnerable to the compromise of integrity, confidentiality an availability of information. As a way forward, the study noted the essence of libraries to implement rigorous and up-to-date antiviral software. The study further noted the importance of training and development in order to ensure that management systems are created, implemented and managed accordingly to ensure security. In addition, the study noted the essence of formulating information security policies and procedures conforming to the BYOD facility.*

Keywords: Information Security, Integrity, Confidentiality, Availability, Public Libraries

Introduction

The Information Communication Technologies (ICTs) in public libraries has had a huge impact on security issues. In other words, such libraries have been vulnerable to diverse information security threats, which compromise the confidentiality, integrity, and availability of information resources. The impact of such information security in public libraries has also extended to the societies that the public libraries serve. Particularly as such libraries have an ethical responsibility to ensure information controls and protection of their holdings for the benefit of all stakeholders, that is, all entities and groups that have a stake in, or claim on the public library. Such stakeholders typically comprise of the public library's shareholders, personnel, patrons, suppliers, general community, other libraries, government agencies, and special-interest groups. The effect of such information security threats has been mostly profound in developing countries, as they have had difficulties in ensuring effective information controls. Therefore, the

tenet of this study was to assess the information security challenges faced by public libraries in a developing country, that is Zimbabwe, through a case study of the Masvingo City Center Public Libraries, given the implementation of diverse information resources (ICTs) in these libraries.

Review of Related Literature

In the modern era, most public libraries in developed countries have become aware of the essence of keeping all their informational resources, virtual as well as physical, secure from within and without threats. According to Mcleod & Schell (2007) when institutions first became aware of the need to ensure information security, their attention particularly focused on protecting hardware and data resources, with the term system security being coined. However, this narrow focus was eventually expanded to encompass not only hardware and data, but also computer facilities, software, and persware (individual users). Mcleod & Schell (2007) posit that currently, the scope of information security has broadened to include any given type of data, not just computer based. As such information security describes the protection of computer and non-computer resources, equipment, facilities, data, and information from misuse by unauthorised individuals. Guvava & Madziwo (2011) elucidate that information security corresponds to the process of protecting data from unauthorised access, disclosure, use, modification, destruction, or disruption. It is focused on the confidentiality, integrity and availability of information irrespective of the form, electronic, print, or other forms. Mcleod & Schell (2007) note that in terms of confidentiality, an organisation will be endeavouring to protect its data and information from access or disclosure to unauthorised individuals. Guvava & Madziwo (2011) were of the view that public libraries should have in place systems and procedures that repel unauthorised access. Adhering to integrity, Mcleod & Schell (2007) denoted that all information systems should be able to provide an authentic and accurate representation of the physical systems that they connote to or represent. In their view, the essence of any given organisation's information infrastructure is to enable its data and information to be available. As such information security is also concerned with the availability issues in an organisation's holdings. Chiwundura (2017) contends that public libraries should be able to ensure that its information and associated services are accessible (available) to all authorised patrons and users whenever required.

There are several information security threats that can compromise the confidentiality, integrity and availability of information in public libraries. Laudon & Laudon (2012) expound that an information security threat conforms to an individual, institution, mechanism, or event that has a potential of inflicting harm upon an organisation's information resources. According to Newton (2010) as public libraries are open to any given individual, hence they are vulnerable to users gaining unauthorised access, modifying institutional documents or causing harm to the library networks. Public libraries make use of large public networks extensively, such as the internet, hence making them more vulnerable, as they are virtually open to anyone. Ismail & Zainab (2011) note that some public libraries have been vulnerable to systems malfunction, were computer hardware are likely to break down, were they are not configured appropriately, or damaged by inadequate use or criminal acts. In addition, Newton (2010) connotes that errors in programming, inappropriate installation, or unauthorised alterations can cause computer software to fail. Power failures, fires, floods, or other natural disasters can also interrupt computer systems. Laudon & Laudon (2012) denote that malicious software programs include a variety of information security threats, such as worms, computer viruses, and Trojan horses. Kahn (2003)

clarifies that diverse web 2.0 applications, such as wikis, blogs, and social networking sites such as Twitter, Facebook and Myspace, have emerged as new conduits for malware. These applications permit users to post software code as part and parcel of the permissible content, and such a code can be launched automatically once the Web page is viewed.

Several public libraries, mostly in developing countries, have difficulties in addressing the information security threats. Sanaman & Kumar (2014) posit that most librarians often get stuck in technological mud. In accord, Singh & Margam (2018) add that generally, there are wide array of technologies that can be acquired or installed by organisations, as such, most organisations end up acquiring technologies that are irrelevant to their informational resources. A study by Ncube (2016) found out that lack of training and development on the part of the library staff members affected the technical expertise in addressing information security threats. Laudon & Laudon (2012) explicate that there are information security technologies that are relatively expensive, making it difficult for some libraries to acquire them. Mugo (2013) reveals that most public libraries depend on subscriptions from patrons, which are usually not enough for their day-to-day operations, thus making it difficult for them to acquire or subscribe to adequate information security technologies. McHale (2017) submits that lack of planning affects the acquisition and installation of information security technologies and resources. Hence, due to lack of plans, it becomes difficult for the libraries to effectively put in place adequate security for their information and holdings.

In view of the information security threats that public libraries are vulnerable to, there are several controls that can be set up to protect informational resources. According to Laudon & Laudon (2012) controls correspond to methods, procedures, and organisational policies that warrant the safety of the organisation's assets; the accuracy and consistency of its information and records; and functional adherence to management principles. Reed (2015) promulgates that public libraries can make use of physical protection using physical barriers, which are envisioned to protect the informational resources against unauthorised access and theft. The reasoning behind this control is that if access to equipment and rooms is restricted, threats of theft and vandalism are reduced. Laudon & Laudon (2012) pronounce that locks, security personnel, barriers and security chains are typical examples of this form of control. Conforming to biometric controls, Singh & Margam (2018) propounds that these make use of unique features of individuals in order to check and restrict access to sensitive information or equipment. In public libraries, Mugo (2013) indicates that barcode scanners in entrances are the most profound biometric controls. While in some quarters of public libraries there are controls that check fingerprints, voice prints or even retinal to access library staff or administrative computers. According to Laudon & Laudon (2012) passwords, user access privileges and user validation routines are common types of communication controls. Such controls are also used in public libraries to access information resources, like computers, and to gain access to certain databases of information within the libraries. Singh & Margam (2018) illuminate that public libraries must have up-to-date and effective antiviral software programmes, as the libraries are anticipated to ensure that patrons make use of external devices, like flash drives, in the libraries. In addition, patrons also gain access to library networks through Wi-Fi connection, as such antiviral software programmes are imperative. Reed (2015) advocates for the formulation of a comprehensive information security policy as an effective control in public libraries.

Research Questions

The following are the research questions that guided this study:

- How are public libraries in the city of Masvingo vulnerable to information security threats?
- Why are public libraries in the city of Masvingo having difficulties in ensuring information security?
- How can public libraries in the city of Masvingo enhance information security controls?

Study Methodology

The research was undertaken at the city of Masvingo, with precise emphasis on public libraries within the city. The city of Masvingo had four public libraries, operating under the banner Masvingo City Center Public Libraries. The libraries included Leisure Public Library, Mucheke Public Library, Rujeko Public Library and Chesvingo Public Library. However, due to lack of ICTs at Chesvingo Public Library, the study did not conform to this library. In addition, as the study was mostly interested in information security in accord to ICTs, hence other elements on information security that did not correspond to ICTs were not looked at. The study made use of the qualitative methodology, which was naturalistic, through a case study design of public libraries in Masvingo city center. This was undertaken in order to gain an in-depth understanding of information security in public libraries within this city. This research methodology and trajectory was crucial in establishing perceptions, opinions, and experiences of the study participants.

Expert sampling was used to select five libraries' staff members from the libraries. The same sampling technique was used to select two libraries' committee members, and two Zimbabwe Library Association in Masvingo Province representatives. Basically, the study made use of purposive sampling, entailing study participants being selected intentionally based on their understanding and knowledge regarding public libraries and information security. Patton (2002) expounds that the rationality and supremacy of purposive sampling rests in the selection of information rich participants for an in-depth study. Captive sampling technique was used to select nineteen libraries' patrons from the libraries. This sampling technique entailed selecting participants that were available and accessible during the time of data generation. Saturation was reached upon administering nineteen questerviews to the libraries' patrons. Interviews with libraries' staff members, libraries' committee members, and members of the Zimbabwe Library Association in Masvingo Province, afforded valuable information to answer all the research question. Questerviews from the libraries' patrons provided information on the first and last research questions. Questerviews are generally homogeneous self-completion questionnaires and questions, during in-depth interviews as noted by Adamson, Gooberman-Hill, Woolhead, and Donovan (2004). The study also made use of observations to have a clearer picture of the study. To analyse the data, the researcher used the Nvivo software. This is a qualitative data analysis (QDA) computer software, which is designed for qualitative researchers, working with extensive rich text based (QSR International, 2015). This software afforded a better appreciation of unstructured data, and allowed the researcher to sort, categorise and organise the data according to their relationships and themes. The qualitative data was presented using words, themes and verbatim quotations as emanating from Nvivo.

Research Findings and Discussions

This section was divided into three subsections. The first subsection looked at how the public libraries in the city of Masvingo are vulnerable to information security threats. The second subsection focused on why such public libraries were finding it difficult to ensure information security. The last subsection focused on how these public libraries could enhance information security controls.

Vulnerability to Information Security Threats

Information obtained from the libraries' staff members revealed that the libraries were vulnerable to unauthorised access to sensitive information and networks. The following sentiments were noted by one of the libraries' staff members:

The library does not have state of the art access control mechanisms to prevent promiscuous patrons from accessing library documents through the network, and the library network does not have adequate security controls to prevent individuals from gaining access to the network. As such the library is exposed to unauthorised access. In addition, the Online Public Access Catalogue (OPAC) also brings about security challenges, as patrons and other individuals can access the library's informational resources from external or remote sites. Thus, exposing the library to unauthorised access.

Questerview findings from the libraries' patrons also revealed that individuals were able to gain access to the libraries' network using diverse hacking software, as the libraries had not put in place adequate access control mechanisms. In addition, the researcher also observed that several individuals streamed with their laptops and cell phones along the peripherals of the libraries during the libraries' operational hours and after libraries' closure to gain access to the libraries' network. As such, the public libraries were vulnerable to unauthorised access, in accord to the sentiments noted by Newton (2010).

In addition to the above finding, the libraries' staff members and libraries' committee members cited that the networks have been vulnerable to denial of service due to congestion. In other terms, patrons and libraries' staff members are at times unable to gain adequate access to the network due to network congestion, given that the libraries' network does not have adequate controls. Most of these participants noted that the bandwidth of the libraries' network was relatively low, while access controls to the network were ineffective. This had led to congestion in the network, with the resultant being denial of internet service to diverse libraries' stakeholders. The researcher also observed that patrons and staff members within the libraries spent a considerate amount of time to open a single web page. Thus, denial of services was another security threat that the public libraries were vulnerable to, in harmony with the viewpoints suggested by Laudon & Laudon (2012).

The researcher observed that the computer resources within the libraries did not have user privilege controls. Such that patrons logged in the computer resources through the administrator access privileges. This entailed that the patrons could install or alter any program within the computers with restrictions. Commenting on this aspect, the ZIMLA representative explained

that lack of user account privileges not only exposed the libraries to the modification of their programs, but also exposed the computers to damage as individuals could install programs that could damage the computer resources. One of the ZIMLA representatives was also of the view that the public libraries were vulnerable to litigation, as individuals could install programs that require licensing, with the public libraries being litigated for the installation without a licence. In addition, the individual noted that there are certain censored programs, mostly those with adult or pornographic content, as such, patrons can easily install such programs and expose the libraries to diverse litigation and ethical consequences. The libraries' staff members and libraries' committee members attributed this vulnerability to lack of an ICT dedicated employee, possessing ICT related skills and competencies to manage the ICT resources and equipment in the libraries.

The libraries were also vulnerable to virus attacks, as the computer resources did not have adequate antiviral software. Information obtained from one of the libraries' staff members revealed that the libraries did not have effective antivirus software protection. The following were some of the opinions alluded to by the participant:

The library mostly uses free antiviral software that does not come about with several options and effective protection. Some computers that are not connected to the internet have out-dated databases that are now unable to provide effective protection. While some of the computer do not have antivirus software at all. This exposes the library computer and network resources to diverse viral attacks, given that patrons and staff members bring external drives and insert them to the computer resources. While some patrons and staff members also conform to websites that can bring about viruses.

Information obtained from the libraries' patrons also validated this, as they noted that they can insert external drives, like USB flash drives and external hard drives to the computer resources. Therefore, the public libraries are exposed to computer and network viral attacks due to lack of effective and adequate antivirus software (Johnson, 2003; Kahn, 2003; Laudon & Laudon, 2012).

As the libraries had institute the Bring Your Own Device (BYOD) concept, with patrons and libraries' staff members given the mandate to bring personal devices and gadgets to the libraries. This facility exposed the libraries to diverse security issues. Interview findings with the ZIMLA representatives indicated that as public libraries extended their service provision by allowing patrons to bring and use personal devices in the holdings, there are security challenges and vulnerabilities. These include damage to the libraries' computers as patrons attach USB devices, earphones and other devices, and damage to the libraries' electric sockets and adapters as patrons make use of them to attach their devices. In addition, the libraries' staff members indicated that some patrons mishandled the library resources to accommodate personal devices, for example, removing of libraries' computers to place personal laptops on electric sockets and adapters. Thus, the institution of the BYOD exposed the libraries to diverse information security threats (Stanford, 2017).

The study further found out that lack of biometric security controls, like Closed Circuit Television (CCTV) exposed the libraries' information resources to acts of vandalism and theft. The researcher observed that the libraries did not have devices that could monitor activities

within the libraries; entailing that the libraries were vulnerable to acts of vandalism and theft. This was also substantiated by one of the libraries' staff members who signified the ensuing emotion:

Currently all our city public libraries do not have the CCTV technology and detectors. This entails that we are unable to monitor each activity that transpire in the libraries, such that patrons can destroy or steal the ICT resources and succeed without a trace. In addition, the presence of CCTV technology in the library acts as a deterrent agent to any mischief in the libraries.

This entails that lack of CCTV technologies and other biometric security control technologies indicates that the public libraries were vulnerable to vandalism and theft from patrons and other relative individuals.

Information obtained from the libraries' staff members revealed that the libraries did not have network firewalls and data encryptions software. Such firewalls prevent unauthorised access to the libraries' network; while data encryption software disguises data or information such that the data or information would not make sense to an individual without the decryption software for the data or information. In their view, this entailed that the libraries were vulnerable to hackers. This was also highlighted by the libraries' committee members who indicated that as an entity to the Masvingo City Council, the public libraries have access to highly classified and sensitive information pertaining to the council. Hence lack of firewalls and encryption software entailed that they were vulnerable to the threat of hackers, who would want to gain access to information about the libraries and the city. Laudon and Laudon (4) also noted that most institutions without firewalls and encryption software are vulnerable to attacks from hackers, who would want to gain access to sensitive information of the organisation.

The researcher observed that though the libraries had fire extinguishers and firehoses to address the threat of fire, however, they were vulnerable to a number of disasters that could damage the libraries and its informational resources. The libraries did not have lightning conductors, entailing that they were vulnerable to lightning strikes. They also did not have flood harvesters and fire detection systems. This entailed that they were vulnerable to water flooding, and fire destructions. In terms of recovery and backups, information from the libraries' staff members revealed that the libraries had not instituted information recovery techniques and had not backups. One of the libraries' staff members noted the following;

The libraries are aware of the diverse natural disasters that they are vulnerable to, due to lack of redress measures. In terms of recovery after the disasters, the library is yet to undertake a risk assessment and management to institute recovery methods. Also, the risk assessment and management exercise will determine the specific information sets that would need to be backed up.

This entails that the public libraries in the city of Masvingo were vulnerable to natural disasters that could damage the ICT resources and equipment. In other terms, lack of recovery and backup facilities entailed that the libraries were vulnerable to security threats of natural disasters.

Reasons for Difficulties in Ensuring Information Security

Information obtained from the libraries' staff members and library committee members revealed that lack of adequate financial resources was a major difficulty. The staff members noted that a number of effective information security controls required extensive investments of financial resources, which the libraries did not have given that they depended on patrons' subscriptions, which were not enough to cater for operational costs, and a poultry budget from the parent institution (Masvingo City Council). The subsequent was aired by one of the staff members:

In order to provide and enhance security in the library, there is need for the library to purchase or subscribe to certain security resources. These require extensive financial investments, which the library does not have. In other terms, the library is financially incapacitated to ensure effective information security controls. As such, the library mostly resorts to free security resources, like free antiviral software, which that effective in protecting the computer and informational resources and equipment in the library.

In accord to this finding, Mugo (2013) explains that several public libraries, particularly in developing countries find it expensive to effectively implement diverse information security controls. While Laudon & Laudon (2012) designate that some controls are relatively expensive for some organisations.

Interview findings with the staff members revealed that the libraries were understaffed. Thus, for effective institution of physical control, there is need for staff members. The presence of staff members in designated places where there is usage of ICTs in the libraries can act as deterring agents in accessing unauthorised information or damaging the libraries' ICTs resources. For example, one of the libraries' staff members noted the following:

The library does not operate for long hours due to lack of adequate staff compliment. This lack of adequate staff compliment also impacts on the security of the library. Apart from having security personnel, there is need for library staff members to physically monitor the usage of library computers and network. For instance, it is difficult for library staff members to ensure that patrons do not gain access to websites that mostly come about with viruses, like pornographic sites, through the library network.

The libraries' committee members also revealed that inadequate staff compliments affected the libraries in safeguarding information security. In their view, the libraries lacked an ICT Technician or a Systems Administrator that should oversee all ICT related issues. Thus, the ICT personnel should oversee administering, maintaining and troubleshooting ICT related resources and equipment, with the libraries' staff members focusing on information provision through the ICTs. Thus, inadequate staff compliments in public libraries affects their functionality and operations (Ncube, 2016).

The other difficulty that the libraries face corresponds to lack of a comprehensive information security policy. Findings from the libraries' staff members noted that the libraries are still in the process of establishing an information security policy. One of the libraries' staff members aired the following sentiments:

Overall, the libraries in the city are still in their infancy stage in terms of their functionality. Thus, a number of policies and procedures are yet to be formulated. This includes information security policies. However, the strategic plans of the libraries encompass the establishment of such policies.

While the libraries' committee members cited that lack of a clear information security policy that provides direction, procedures and standards of conformity in relation to the libraries' resources and equipment is a major challenge. One of the ZIMLA representatives also indicated that lack of a clear policy on security issues in the libraries can be a challenge in ensuring security of the libraries' resources and information products. This is in tantamount with Reed (2015) who signifies that lack of information security policies in public libraries affects the security of libraries.

The researcher observed the libraries were having difficulties in managing the BYOD facility. Thus, even though the libraries' patrons were given the platform to bring their own resources to the libraries, for instance, their own laptops, USB flash drives, and cell phones to use in the libraries, the libraries had difficulties in ensuring information security from this concept. Connecting personal devices to the libraries' resources (computers, network, printers, power sockets and other equipment), had brought about challenges. According to the library committee members, while BYOD offers numerous benefits within the libraries, it also presented several security challenges. The following were the security challenges that one of the libraries' committee. Such challenges included unauthorised access, particularly on the libraries' network, noise (as individuals use their devices). Also, in terms of staff members, corporate data were being copied and transferred to personal devices. The libraries' committee members attributed these challenges to lack of a clear-cut policy and standard operating procedure on the implementation of the BYOD concept. This is in line with the notion expression by Stanford (2017), who connotes that lack of adequate policies and procedures can have negative implications on the use of personal devices in libraries.

The other reason for difficulties in ensuring information security within the study public libraries adheres to balancing issues of intellectual freedom and censorship. Interview findings with the ZIMLA representatives indicated that this is a challenge confronting most public libraries. Thus they are supposed to provide access to information as indicated in the Universal Declaration of Human Rights, the Constitution of Zimbabwe, and the National Library Documentation Services (NLDS) Act that governs public libraries in Zimbabwe (intellectual freedom), at the same time restrict access to certain information due to security issues (censorship). The ZIMLA representatives noted that balancing intellectual freedom and censorship is a difficulty confronting the security of public libraries. For instance, when the public libraries censor access to certain information, they are exposing themselves to queries and litigation, thus making it difficult for the libraries to censor information for security reasons.

For effective information security, there is need for skills and competencies on the part of the libraries' staff members on information security. Interview findings with the libraries' staff members and libraries' committee members highlighted that there are training and development needs in information security. One of the libraries' staff members cited the following:

Though the library has skills and competent staff members in the area of library service provision, there is, however, a need for training and development in the area of ICTs. In accord to information security. The institution of ICTs in libraries is a generally new, unique and profound area that has expanded the resource base of the libraries. However, there are security issues that are brought about by these ICTs, which necessitate the library staff members to undertake continuous training and development.

The ZIMLA representatives were in harmony, as they noted that as much as there is continuous changes and developments in ICTs and their usage in public libraries, there is generally a profound training and development gap that exists among staff members. Such that they are unable to staff afoot with the developments, including the area of information security. This finding also connotes with the viewpoint noted by Ncube (2016) that inadequate training and development affects information security in most public libraries within developing countries.

The study further found that lack of management support was another difficulty faced in ensuring adequate information security. The following was noted by one of the staff members:
For effective library services, there is a need for top management support. The library's top management, that is the council, does not adequately provide support for some of the library initiatives. Support should not be limited to finance but should extend to providing all necessary resources and motivation relative to effectively provide library services. This also relates to information security, whereby one would expect such an essential aspect to be a priority to the top management.

This finding correlates to Guvava & Madziwo's (2011) view, that most of the libraries' initiatives are dwindled by lack of top management support.

Information Security Controls

The ZIMLA representatives noted that there was a need for the libraries to undertake a risk management exercise. This would enable them to identify the risks that they are exposed to and devise strategic plans to counter the risks. The representative noted that this risk management exercise would provide a foundation for libraries' resources and equipment audits. In other terms, since the risk management endeavour would entail taking stock of the libraries' resources and equipment, such a move would become a base for audits in the libraries. According to Laudon & Laudon (2012) audits are essential information security controls as they provide information on the state and use of the resources and equipment in an institute. In accord, some of the libraries' committee members noted the essence of a risk management exercise. One of which noted the following:

For the libraries to be able to have a risk register, detailing the risks that the libraries are exposed to, their likelihood, impact and treatment, there is a need for a risk management exercise. Such an exercise is on the cards. In other terms, it is within the libraries' strategic plan to undertake a risk management of the informational and other resources in the libraries.

This entails that a risk management exercise is an essential information security control that the libraries can correspond to.

The libraries committee members noted with concern the need for an information security policy. Such a policy would provide guidelines on issues that correspond to information security. The essence of such a policy was further highlighted by the ZIMLA representatives, who cited that for effective information security within the public libraries, there was a need for the formulation of an information security policy. In their view, such a strategic document would provide strategies of dealing with security issues in the libraries, acting as a referral point for any dilemma or confusion on information security issues. In harmony with this finding, Reed (2015) emphasises the essence of such a policy within public libraries.

Information obtained from the libraries' patrons indicated that the libraries could undertake continuous backup through the cloud. The following was noted by one of the patrons in this regard:

Notwithstanding the challenges that can also come about by using cloud facilities, like google drive, OneDrive, Tumblr and other internet-based facilities for saving documents; however, the libraries can use these facilities to make backups for their informational resources. The advantage of these is that they are managed by other companies around the world, who want to ensure that their integrity is not compromised, hence they provide a number of security measures to protect documents and information. In addition, most of them have free facilities, though with limited features, entailing that the libraries can conform to them if they do not have adequate financial base.

In line with the above sentiments, one of the ZIMLA representatives indicated that there are a number of open source backup facilities found on the internet, which do not require financial investments. In other terms, there are several free, open source backup software that enable cloud saving that the public libraries can adhere to (Walldén & Soronen, 2004).

The other information control mechanisms conformed to the acquisition and installation of antivirus and CCTV technologies. The libraries' staff members noted that it was essential for the libraries to have these technologies in place. Though they cited the financial crises. In addressing such financial issues in order to acquire relevant library resources, the ZIMLA representatives were of the view that the council should enhance its budgetary allocation towards the public libraries. According to one of the representatives, although the council seems to be experiencing financial challenges, relative to the national economy, it is critical for the libraries to liaise with the authority to increase the libraries' budgetary allocation. In other words, the libraries should undertake advocacy to management for effective financial support. Questerview findings from some of the libraries' patrons confirmed this point, as they stressed the need for the local authority to afford financial resources towards the development of the public libraries. In addition, the ZIMLA representatives also narrated that there are a number of donor and financial organisation that could provide financial and resources assistance to libraries and information centres, hence it deemed to be essential for the libraries to adhere to such institutions for donations. This is in line with what Mugo (2013) and Ncube (2016) signify about ways of raising financial resources to acquire library resources and equipment.

Training and capacity development for staff members was also alluded to as an important information security control mechanism. The libraries' patrons noted that most staff members were not adequately skills on ICT related issues, hence the need for training and developing them. The libraries' staff members also indicated that continuous capacity development ICTs and information security issues was significant. One of the staff members noted the following:

It is imperative for the staff members to be trained in this area of ICT. Instead of library staff members assisting patrons in using ICT based resources, you will find that it's the other way around, with patrons helping staff to use the technologies. Hence a need for training and development. In addition, this area of information security is a moderately contemporary subject area within the field and vicinity of library and information science. Entailing a need for continuous capacity development. Therefore, in the libraries' strategic plans, training and development issues are well documented; with diverse individuals identified to facilitate the training and development exercises.

Therefore, as an information security control, there is need for the public libraries to continuously train and develop their staff members (Ncube, 2016).

Information obtained from the one of the libraries' patrons revealed that partnerships are importance for the growth and effectiveness of the public libraries. According to the patron, the libraries should relate to collaborations and partnerships with diverse institutes that relate to library and information provision. One of the ZIMLA representative also noted this aspect through the following were the sentiments:

For the libraries public libraries to edify their effectiveness, including this area of security, they must partner and collaborate with many institutions and association. The public libraries partnered with the Zimbabwe Library Association, which was a great move. Conversely, there is a need for the libraries to expand their horizons per se, by going a step further to partner with other stakeholders in Masvingo particularly, and Zimbabwe at large, in order to share ideas and best practices.

Achitabwino (2007) avows that the success of any public library also rests on the synergies it makes with other players in their domains of influence. Therefore, to certify effective service delivery, including information security, partnerships are vital for public libraries.

Conclusions

In conclusion, the Masvingo City Center Public Libraries are vulnerable to the compromise of integrity, confidentiality and availability to its informational resources and equipment, due to a number of information security threats. The most apparent vulnerability conforms to inadequate access controls to computer and network resources, alongside natural disasters. The libraries are also confronted with several difficulties in addressing the threats that they are confronted with. The most prevalent one corresponds to lack of adequate financial resources that cascade from the national economy, to the Masvingo council, and to the libraries respectively. There are, however, several strategies that the libraries can institute to control the information security threats, with training and development being the urgent issues that needs attention.

Way Forward

As a way forward, there is a need for the public libraries' top management support, which could be exhibited by inviting specialists to train and capacitate staff members on information security issues. The public libraries should also continuous undertake advocacy to the top management, that is the council, on the essence of supporting the libraries' activities and initiatives. The ZIMLA Masvingo Branch could provide strategic direction regarding information security in public libraries. Furthermore, there is need for public libraries to conform to Private, Public Partnership (PPP) with diverse associations and organisations, which include among others, ICT centres, information security companies, banks, Zimbabwe Library Association.

References

1. Achitabwino, P., (2007). *Libraries and national development*. Retrieved from: http://pachitabwino.blogspot.com/2007/03/libraries-and-national-development.htm (accessed 17 September 2018).
2. Adamson, J., Gooberman-Hill, R., Woolhead, G. and Donovan, J. (2004). 'Questerviews': using questionnaires in qualitative interviews as a method of integrating qualitative and quantitative health services research', *J. Health Serv. Res. Policy, Vol. 9*, No. 3, pp.139–45.
3. Chiwundura, P. (2017). *The security of electronic student records*. Gweru: Zimbabwe Open University Midlands Campus.
4. Guvava, N. & Madziwo, M. (2011). *Introduction to computers*. Mount Pleasant: Zimbabwe Open University.
5. Ismail, R. & Zainab, A.N. (2011). Information systems security in special and public libraries: An assessment of status. *Malaysian Journal of Library & Information Science, Vol. 16*, no. pp. 45-62.
6. Johnson, G. (2003). *Exploring corporate strategy: Text and cases*. 6th ed. New Jersey: Prentice-Hall, Inc.
7. Kahn, M., 2003. *Protecting your library's digital sources: The essential guide to planning and preservation.* Chicago: American Library Association.
8. Laudon, K.C. & Laudon, J. P. (2012). *Management information systems: Managing the digital firm.* Boston: Prentice Hall.
9. McHale, J. (2017). *Virtual threats that are all too real: managing the cyber security of buildings will require a coordinated effort among stakeholders in the facilities industry*. Retrieved from https://facilityexecutive.com/2017/08/cyber-security-virtual-threats-that-are-all-too-real/. (accessed 15 September 2018).
10. Mcleod, R. & Schell, G.P. (2007). *Management information systems*. New Delphi: Dorling Kindersley (India) Pvt. Ltd.
11. Mugo, C. B. (2013). *Assistive technology and access to quality instruction for blind and visually impaired students: A comparative study of Kenyatta University, Kenya and Syracuse University, USA*. Retrieved from http://ir-library.ku.ac.ke/bitstream/handle/123456789/9009/Bernard%20Chomba%20Mugo.pdf?sequence=1. (accessed 16 September 2018).

12. Ncube, M.M. (2016). *The impact of the absence of municipal libraries on lifelong learning on the Mkoba community in Gweru, Zimbabwe*. Midlands State University: Dyke.
13. Newton, J. (2010). *Guidelines for automatic data processing physical security and risk management*. New York: Doubledsfy.
14. Parmar, (2007). *Information resource guide: Computer, internet and network systems security*. Duncan, BC: N. Cowichan Duncan RCMP.
15. Patton, M.Q. (2002). *Qualitative research and evaluation methods*. Sage: Thousand Oaks, CA.
16. QSR International, 2015. *Nvivo*. Retrieved from https://www.qsrinternational.com/nvivo/home (accessed 28 September 2018).
17. Reed, G.M. (2015). *Information and records management*. New York, NY: McGraw-Hill.
18. Rojers, D. (2010). *Management systems*. Holt, Rinehart and Winston, Inc.
19. Sanaman, G. & Kumar, S. (2014). Assistive technologies for people with disabilities in national capital region libraries of India. *Library Philosophy and Practice (e-journal)*. Paper 1200. Retrieved from http://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=3127&context=libphilprac. (accessed 15 September 2018).
20. Singh, V. & Margam, M. (2018). Information security measures of libraries of central universities of Delhi: A study. *Journal of Library & Information Technology, Vol. 38*, No. 2, pp. 102-109.
21. Stanford, D. (2017). *Four mobile BYOD & cyber security trends in 2017*. Retrieved from https://bigdata-madesimple.com/four-mobile-byod-cyber-security-trends-in-2017/ (accessed 19 September 2018).
22. Walldén, S. & Soronen, A. (2004). *Edutainment: From television and computers to digital television*. Retrieved from http://www.uta.fi/hyper/julkaisut/b/fitv03b.pdf. (accessed 15 September 2018).
23. Yamson, G.C. (2016). *Assessments of collection security management in academic libraries: A case study of Central University Library*. Retrieved from https://eujournal.org/index.php/esj/article/viewFile/8623/8253. (accessed 22 September 2018).