Library Hi Tech

Digital disaster management in libraries in India
Parul Zaveri

Article information:

To cite this document:
Parul Zaveri , (2015),"Digital disaster management in libraries in India", Library Hi Tech, Vol. 33 Iss 2 pp. 230 - 244
Permanent link to this document:
http://dx.doi.org/10.1108/LHT-09-2014-0090

Digital disaster management in libraries in India

Parul Zaveri
SHPT School of Library Science, SNDT Women's University, Mumbai, India

Received 4 April 2014
Revised 10 February 2015
Accepted 21 February 2015

Abstract

Purpose – Disaster management is an issue that has received relatively little attention in libraries, particularly in India. With the growth in digital resources in libraries, it is necessary for librarians to understand and apply the ways of protecting digital data and the related equipment from disaster. The purpose of this paper is to address the issues related to digital data protection in libraries in India. It aims to investigate the perceptions of librarians about the probability of digital disasters happening in their libraries, and to assess the level of digital disaster preparedness among libraries.

Design/methodology/approach – A questionnaire based survey of 276 libraries in the Western region of India was conducted to find out the digital data protection measures taken by them. The paper provides an overview and analysis of the general trends in digital data protection in these libraries.

Findings – The research results indicate that due to lack of knowledge about handling of digital data, and inadequate digital infrastructure setup in organizations, the chances of loss of digital data are high. However, common measures like taking backup of data manually are mostly followed by all libraries. The paper has identified the trends in protection of digital data, as well as the lacunae, in Indian libraries. Basic guidelines on digital data preservation are also presented in the paper.

Practical implications – The guidelines provided in the paper will be useful to any libraries to take measures for protection of the digital data. The libraries will be able to prepare their digital data protection plan and train the staff accordingly.

Originality/value – This paper is the first to address the issue of digital disaster management in libraries in India. It provides a detailed analysis of digital data protection measures taken by Indian libraries currently.

Keywords Data backup, Digital data disaster, Digital data management, Digital data preservation, Library disasters

Paper type Research paper

Introduction

Libraries in India today are in a hybrid state, as traditional print-based collections collected over many years are being supplemented by digital collections which are being acquired and added into the collections. Libraries are acquiring born digital materials and also creating in-house digital resources. Further, library collections include e-books, e-journals, e-theses and dissertations. Many libraries maintain the institutional repositories of the parent institutions. Information and communication technologies have completely changed the nature of the collections, the functioning of libraries and the services offered. Library functions are automated using open source or commercial software. Libraries are networked and connected through telecommunication networks. Libraries have uploaded web sites and often created blogs for users. Web OPACs of many libraries are searchable on the internet. These are all managed by professionally qualified librarians who may not be IT specialists.

Any neglect, damage or destruction of library resources carries with it grave consequences for the parent institution and for society at large. It not only results in economic losses but also affects the cultural identity and legacy for the future, disrupts the education processes and systems, and sets back knowledge creation. It thus

Library Hi Tech
Vol. 33 No. 2, 2015
pp. 230-244

0737-8831
DOI 10.1108/LHT-09-2014-0090

becomes imperative to ensure that the risk to libraries from all kinds of disasters is minimized, in particular digital disasters.

It is believed that most libraries in India have given comparatively little thought to disaster preparedness. This is reflected in the professional literature, and has also been convincingly demonstrated in the doctoral research conducted by Zaveri (2013). The present study derives from and extends on this research, but focuses specifically on disaster preparedness for digital disasters.

Background

The Oxford English Dictionary defines disaster as "anything that befalls of ruinous or distressing nature; a sudden or great misfortune, mishap, or misadventure; a calamity" (Disaster, 1989, p. 713). It is an occurrence arising with little or no warning. It usually occurs suddenly and the impact may be experienced over a long period. The probability of occurrence of a potentially damaging phenomenon within a certain time frame is referred to as a hazard. Vulnerability, on the other hand, refers to how susceptible a place is. Risk refers to the probability that loss will occur as the result of an adverse phenomenon happening. Based on mathematical calculations, risk (R) is the product of hazard (H) and vulnerability (V); $R = (H) \times (V)$ (Raghavan *et al.*, 2009).

Disaster management is the body of policy and administrative decisions and operational activities which pertain to the various stages of a disaster at all levels (United Nations Development Programme and United Nations Disaster Relief Organization, 1992). It is a systematic process which is based on the key management principles of planning, organizing, leading, coordinating and controlling. As Kofi Annan, Secretary General of United Nations succinctly commented "while the costs of prevention have to be paid in the present, its benefits lie in a distant future. Moreover, benefits are not tangible; they are the disasters that did *not* happen" (International Federation of Red Crescent Societies, 2002, p. 15). A digital disaster can be defined as loss of digital data which is required for business continuity operations 24/7. Without this data the functioning of business will stop. Corruption of the data, hardware and software required for critical business operations is considered as digital disaster.

IT disasters in libraries could be due to any of the following:

- fluctuation in power supply;
- power outage;
- software or hardware malfunctions;
- computer viruses;
- hacking of data;
- human errors like spilling of liquids;
- improper computer shutdown; and
- accidental deletion of data.

Moreover, other types of disasters such as fire, flood, vandalism, etc. could also damage the IT infrastructure, resources and services:

> Any digital material loss could be colloquially termed a "disaster", depending on the importance of the digital material, how much it would cost to recover it, and if it is recoverable at all (Rinehart *et al.*, 2014).

The disaster management cycle consists of the following main stages:

(1) mitigation: it is achieved by taking long term preventive measures after risk analysis;

(2) preparedness: this is usually regarded as comprising measures which enable organizations, communities and individuals to respond rapidly and effectively to disaster situations;

(3) response: response measures are applied immediately after the disaster, e.g. implementation of plan, activation of counter-disaster system, search and rescue, etc.; and

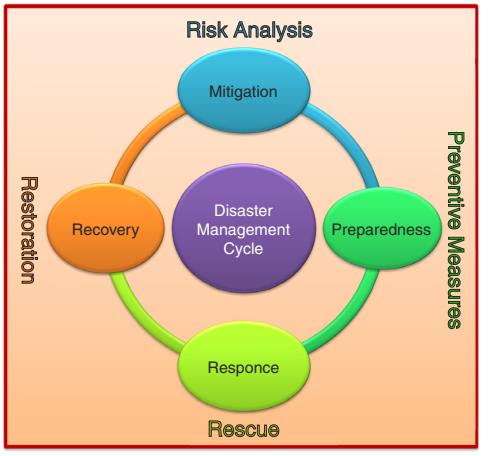
(4) recovery: the aim of this phase is to restore the affected area to its previous state (Figure 1).

Review of literature

Digital disasters can occur in parallel with natural or man-made disasters or can happen of their own accord. The status of preservation of digital resources and disaster recovery measures taken by libraries in China were studied by Jiazhen and Daoling (2007). Findings indicated that physical deterioration of data led to non-renewable data loss, inability to read the data due to obsolete storage media, weak data back-up management system, shortage of relevant knowledge on preserving digital information resources and failure to migrate the obsolete data in time.

A comparative evaluation among three main cultural institutions in Malaysia regarding long term preservation of digital content is presented by Manaf and Ismail (2010). To avoid digital disaster, issues relating to hardware and software compatibility, long-term storage, organization of files for ease of search and retrieval, media quality, disaster recovery and integrity of original data have to be kept in mind.

Hawkins *et al.* (2000) have highlighted issues related to prevention and recovery from digital disasters. The authors explain the need to have a disaster recovery plan and discuss how to cost it. They also stress the issue of insurance and training of



Source: Zaveri (2013)

Figure 1.
The disaster management cycle

human beings. Tennant (2001) describes how to cope with disasters in digital libraries and what preventive measures should be taken to avoid disasters. Boss (2002) also explains how a proxy-server and firewalls can protect the database server of a library. Georges (2004), emphasizes issues related to having properly trained staff, types of servers to have, backup of data, damage assessment and recovery and restoring operations.

According to Robert Fox (2006), although libraries may assign responsibility for information security to a person or department, it is important for everyone to be aware of the potential risks involved in the security of digital data. There is a need to preserve and guard digital content, prevent digital infiltration and protect electronic infrastructure in a digital library as it is open to the public. Digital librarians need to be familiar with basic web application security because library services and content are being distributed on the web. Fox also describes the types of threats that can be faced in a digital library environment and the necessary security arrangements to be made.

Post 9/11 the need for organizations to be prepared was highlighted. Dimattia (2001) explains the need to have necessary information in duplicate locations including on portable devices. System backups for the organization should also be stored off-site. Every library and information centre should think of the business continuity process in case of emergency.

Jiazhen and Peng (2009) highlighted that due to lack of the demand analysis of Digital Records Management and Business Process Management, the preservation of digital data is affected in the long term. Archival data requires long term preservation and the difficulties faced concern updating of storage media, information transfer and shortage of disaster recovery management plan. According to the authors, in the context of deterioration of the natural environment and the globalization of terrorism, prevention of disaster is extremely significant. Creation of an "e-government disaster recovery centre" is suggested. The recommendations given by Al-Badi *et al.* (2009), with reference to cyclone Gonu which hit Oman in June 2007, are useful for preparedness of IT departments in both public and private sectors. According to Kostagiolas *et al.* (2011) disaster management for digital data is an ignored activity among libraries in Greece.

According to Yoon and Kim (2013) computer security involves protection of digital data and computer hardware from any threat. Threat due to various disasters is one of the managerial issues in any organization. Organizations are introducing security technologies such as secure networking protocols, intrusion detection techniques, database security methods, etc., to reduce and prevent computer security incidents. Computer security is not just related to use of technological tools but also involves user's awareness and behaviour to prevent computer security incidents.

The authors Oehlerts and Liu (2013) have covered various digital preservation practices followed in different countries and insist that for digital data protection against all kinds of damage, every library must have digital preservation policies.

According to Zainab *et al.* (2013) virtual machines provide better solutions for backup and disaster recovery. The paper by Dec˘man and Vintar (2013) suggests a new solution for short- and long-term digital preservation for the public sector with the idea of a centralized digital preservation repository in the form of a community cloud, available to all public administration organizations. Sidorko and Lee (2014) also suggest planning of a collaborative and cooperative central storage facility for Hong Kong academic libraries for protection of digital data.

The digital emergency preparedness and recovery plan for the Paul V. Gavin Library by Illinois Institute of Technology (2012) discusses important issues for being prepared for any kind of digital disaster. In case of disaster, the library should plan, be prepared and develop recovery strategy to preserve the digital data. The disaster plan should describe the long-term preservation strategy of the digital collections, institutional repository and other digital files and records maintained by the library.

Some actual instances of digital disasters have been reported. A week long power failure in 1998 seriously impacted services of the 13 libraries on the campus of the University of Auckland, New Zealand (Grant, 2000). After an AC outage, the server of Montclair University Library did not restart as the aging server equipment did not have automatic temperature control, no documentation was done for restoration of system, and no testing of restoration of data backup was done (Mallery, 2012).

Objectives

The objectives of the research reported here were:

(1) to find out the perceptions of Indian librarians about the probability of digital disasters happening in their libraries;

(2) to assess the level of preparedness for digital disasters among Indian libraries; and

(3) to develop guidelines for digital disaster management in Indian libraries.

Methodology

To meet the study's objectives it was required to approach a large number of libraries of various types. The survey method, which has been described as a non-experimental, descriptive research method, in which information is gathered through written questioning was considered most suitable for the present research (Sarantakos, 2005).

A self-completion questionnaire was prepared as the major tool for data collection. The draft questionnaire was tested for relevance, clarity and simplicity by sending it to select libraries for pilot testing, review and comments. Based on feedback received, modifications were made in the questionnaire. The final questionnaire was sent to university libraries, college libraries, public libraries, and special libraries from the Western region of India, covering three states of India namely, Maharashtra, Gujarat and Goa. A total of 430 questionnaires were sent to various libraries in the region. Out of 430 libraries, 276 libraries (64.18 per cent) responded to the questionnaire (Table I).

Data were analysed using MS-Excel. Based on the feedback received in the questionnaire and published literature, digital disaster management guidelines have been prepared for Indian libraries.

Table I. Questionnaires sent and responses received

Type of library	Questionnaires sent	Responses received	% of responses
University libraries	62	53	85.48
College libraries	227	134	59.03
Public libraries	41	24	63.16
Special libraries	100	65	65
Total	430	276	64.18

Findings

Collections

In the current study, it was found that paper based resources still form the major part of the collection in most of the responding libraries. The responses to the question on type of collection had shown that 218 (78.99 per cent) libraries had more than 90 per cent of their collections in paper based format and 173 (62.68 per cent) libraries had less than 10 per cent of their collections in the digital format.

Overall findings indicate that use of information and communication technologies is growing in all types of libraries. This has become possible due to financial support provided by the University Grants Commission, Government of India, through the Information and Library Network Centre, located at Ahmedabad, to university libraries in India. Also performances of academic institutions in India are assessed by the National Assessment and Accreditation Council. One of the components for assessment by them is the libraries of these institutions. Due to this many libraries today have established an IT infrastructure. Readers of the current generation are Google users and smart phone users. They want information at any time at any place. To meet their expectations, and harnessing the changing publishing scenario from print to electronic resources, libraries are acquiring more digital resources and more computers and setting up computer networks to provide better services to readers.

Hardware and software infrastructure

When asked about the number of computers available in libraries, it was observed that 75 per cent of university libraries, 41 per cent of college libraries, 30 per cent of special libraries and 20 per cent of public libraries had more than 15 computers. Five libraries did not have any computer and about 55 per cent libraries out of 276 libraries had less than ten computers (Figure 2).

Out of the 271 libraries that had computers, 50 (18.45 per cent) libraries had one book scanner, 138 (50.92 per cent) libraries had a printer cum scanner, 248 (91.51 per cent) libraries had at least one printer and 110 (40.59 per cent) libraries had bar code reader and scanner. This shows that libraries are equipped with IT infrastructure which needs to be maintained and upgraded at regular intervals.

In all, 193 (71.22 per cent) libraries were using library automation software like Software for University Libraries, LIBSYS, System for Library Information Management, Library Management Suite and Koha. 220 libraries had internet access in the library. In total, 150 libraries had web site presence as part of the institution web site. Almost 90 per cent libraries had antivirus software installed on their computer systems. Five libraries had installed a radio-frequency identification (RFID) system.

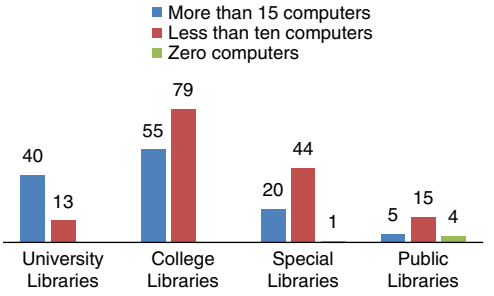


Figure 2.
Number of computers available in libraries

It is concluded that while the building up of IT infrastructure and digital resources is at a beginning stage, it is expected to grow in quantity and sophistication, due to the growing IT penetration in all sectors in the country, and also due to user needs and expectations. Therefore, while librarians are expending considerable effort, time and financial resources on expanding their digital resources and services, they need to simultaneously address the issues of preparedness for digital disasters and particularly data protection.

Opinions of librarians regarding probability of digital disasters

The respondents were asked to indicate their opinions on the probability of disasters occurring in their libraries. The responses are shown in Table II.

The results of the study indicated that just over 50 per cent of the librarians perceived less than 20 per cent chance of digital disaster, while only 7.61 per cent perceived a probability of over 60 per cent. This could be due to various reasons.

First, in most libraries the proportion of digital resources is relatively low compared to print resources. The responses to the question on type of collection in the surveyed libraries had shown that 218 (78.99 per cent) libraries had more than 90 per cent of their collections in paper based format and 173 (62.68 per cent) libraries had less than 10 per cent of their collections in the digital format. There were a few exceptions to this, e.g., Diamond Management & Technology Consultants (India) Library; Mumbai had 100 per cent digital collection which also included online access to databases. Tata Memorial Hospital Library, Mumbai and Shyam Narayan Memorial Library at Thakur College of Engineering & Technology, Mumbai also had 85 and 90 per cent, respectively of their collections in digital format.

Many libraries are still to develop adequate IT infrastructure, and have not addressed long-term issues of preservation and protections. Also it is likely that there is inadequate knowledge among them about preservation and protection of digital resources.

Disaster preparedness

Disaster preparedness and management for digital disasters involves two groups of issues, i.e.:

(1) protection; and

(2) recovery from loss, destruction, failure or obsolescence.

Since the IT infrastructure and services are dependent on power supply, libraries have to address the issue of providing uninterrupted power supply and of dealing with power failures. This is particularly important in places which have regular power outages for load shedding. Regarding the protection of hardware and software, routine maintenance activities are essential.

Table II.
Opinion of librarians on probability of digital disasters occurring in their libraries

Perceived probability	No. of libraries	Percentage of libraries
60% and above	21	7.61
Between 20-59%	92	33.33
< 20%	139	50.36
Not answered	24	8.70
Total	276	100

For digital data, the most fundamental form of preparedness is to safeguard it by taking regular backups.

Further, in case of a disaster that affects the whole library, and not just the digital resources (e.g. fire, flood, etc.), it is useful to have a plan for saving the equipment and the data. Fire and water both can damage the digital data as well as hardware and software available in a library. When a disaster strikes, the electrical power supply to computers must be switched off immediately. Computers should be moved away from windows and walls from where there is greater chance of damage. The cable supplying power to the computer should be removed from the power socket. The computer server room should be protected against fire and leakage. Depending on the level of damage, preventive actions can be planned, e.g. if soot has spread on the hardware, a complete cleaning of hardware should be done. If it is damaged due to water, it should be allowed to dry naturally.

The questionnaire included questions to elicit information on these forms of disaster preparedness.

Power supply

Out of 271 libraries only 142 (52.40 per cent) libraries had uninterrupted power supply to their computer systems. In case of fire or short circuit only 138 (50.92 per cent) libraries out of 271 respondents had automatic tripping of electrical systems. Checking and maintenance of electrical equipment was done by 173 libraries (63.83 per cent).

Protection of hardware and software

It was found that hardware maintenance was done by 80 per cent of libraries. An annual maintenance service was hired by these libraries for hardware care and repair. Physical cleaning of the computer was done by all the libraries.

Of the respondent libraries which had computers, 243 (89.66 per cent) libraries reported that they had antivirus software, while 157 (57.93 per cent) had firewall installed on their computer systems.

No digital data protection policy existed with any respondent library.

Backups

Backups are the only way data can be recovered in case of loss. When asked how important digital backup activity was as part of digital data disaster management, 241 (87.32 per cent) librarians rated it as a very important activity. Compared to their opinion, only 216 (78.26 per cent) respondents took backups.

Frequency of backup and location of the backup files become important considerations, to be able to use the backups. Out of the 271 respondent libraries which had IT infrastructure, 55 (20.30 per cent) took neither manual nor automatic backups, while 216 (79.70 per cent) respondents took backups. Out of those 216, 192 respondents took manual backups and 118 respondents took automatic backups. The overlap of 94 consisted of those libraries which took manual as well as automatic backups. Of the 216 libraries, 137 (63.43 per cent) libraries took backups daily (Table III).

The findings relating to storage of backups show that 128 (59.26 per cent) of the 216 respondents took backups on the same computer at the library while in 131 (60.65 per cent) cases backup was done on another computer in the library. This shows that 43 libraries kept backups on two computers in the library. Backups can be taken

on different computers but if a digital disaster strikes a computer, backup on the same computer is of no help. Similarly, if the disaster strikes all computers in the library, backup done on another computer in the library is of no use. As shown in Figure 3, 81 (37.50 per cent) libraries kept backups on different computers outside the library but within the institution.

Backups on external media were maintained by 153 (70.83 per cent) of the 216 libraries. The external media used for backup were external hard disk, CD, DVD and pendrive. Out of 153 respondents, these external media were stored either in the library – 91(59.48 per cent) or outside the library but within the institution – 47 (30.72 per cent) or outside the institution – 6 (3.92 per cent) or at multiple locations – 28 (18.30 per cent). Backups need to be regulalrly checked to ensure that they are functional and can be restored. Only 155 (71.76 per cent) libraries out of 216 regularly checked the functionality of the backup.

Items for saving

Of the 271 respondent libraries which had computer setup in their premises, it was noteworthy that almost 110 (40.59 per cent) respondents identified computers and peripherals as important items for saving in case of disaster. It is not clear whether this is because of the hardware, software or data on the computer. It may be noted that since many librarians have acquired a computer system after many years of struggle, they consider it to be a very valuable asset. Only about 38 (14.02 per cent) respondents identified digital data backups as one of the items for saving. The findings indicate that compared to paper based records digital data is still less in quantity, so less priority is given for saving of digital backups.

Data backups	Type/frequency	Libraries No.	Libraries %
Type of backups	Manual	192	84.42
	Automatic	118	52.38
Frequency of backups	Daily	137	63.43
	Weekly	80	37.04
	Monthly	61	28.24
	Occasional	37	17.13

Table III.
Types of backups and their frequency

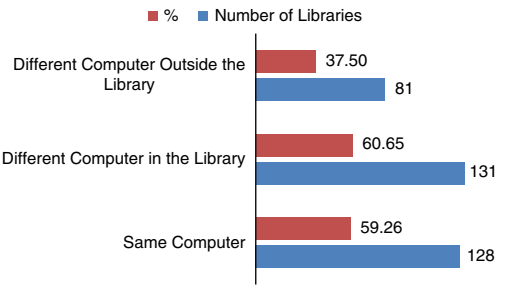


Figure 3.
Storage of backups

Instances of digital disasters

Among the responding libraries, only two (one college and one special library) reported having experienced minor digital disasters. In the year 2008, the College library reported that a desktop PC in its network which was used as a server completely crashed due to frequent power failures. The library automation software was lost and data containing entries for about 40,000 documents was corrupted. Within a week's time a new high end computer was bought to function as a computer sever. As the software was under annual maintenance contract, it was re-installed and the network was re-configured. Luckily the library had a backup on a pen drive and the librarian was able to restore the data. Since this backup was one month old, data for 200 entries was lost completely and this data had to be re-entered.

In 2009 at a multi-national company library in Mumbai with branches all over the country, the library software could not be accessed over the network. It took the company three months to diagnose that the problem was not with the software but in the network. Inadvertently the IP address of the machine on which the software was loaded had been changed. Each and every computer in the network had to be examined before this machine could be located. Till then the library's working was affected. The damage could have been worse since the company had no backup. As it was, the damage was limited to stoppage of services for some time.

These instances should serve as an alarm signal to all libraries. Disasters occur without warning, and disaster preparedness is a necessity.

Guidelines for digital disaster management in Indian libraries

In the light of the growing collections of digital resources, it is essential for Indian librarians to:

- be sensitive to the issues of digital disaster management;
- reduce the risks of digital disasters in their libraries;
- be prepared to deal with a digital disaster should it occur in the library; and
- cope with recovery and restoration processes after a disaster.

The following recommendations are made.

Sensitivity to the issues of digital disaster management

Disaster management, including digital disaster management, should be considered as an integral part of library management. This should be reflected at institutional level in library policies, and at the level of the profession in the literature and in library and information science education.

Reducing the risks of digital disasters in libraries

According to Rothstein (1998), monitoring the vulnerability will prevent a problem before it occurs. The author has listed the main areas of vulnerability (as cited in Hawkins *et al.*, 2000, p. 227).

Certain good practices to be followed in managing IT, which would help to limit the effects of a digital disaster, have been listed by Hawkins *et al.* (2000) and Kahn (2010). Based on suggestions given by authors and by the respondents in the study, the following check list has been prepared. It can be used as a guideline to prevent damage to the digital collection as well as be prepared for digital disaster:

- Taking digital backups. There should be set procedures for taking backups regularly. The responsibility to take backups must be assigned to a person and the person responsible for taking backup must be given appropriate training.
- Care and up-gradation of IT equipments.
- Storing digital data in a fire proof vault.
- Installing RFID, fire wall.
- Having a centralized repository of software.
- Keeping the main switch outside the library, to disconnect in case of emergency.
- Instead of buying assembled computers libraries should acquire hardware and software from reputed and standardized companies.
- Checking if master copies of all software with the respective license keys are stored at a safe location.
- Assigning the annual system maintenance to IT vendors and updating it regularly.
- Keeping uninterruptable power supplies connected to key servers and equipments.
- If libraries have a computer network in the premises, a detailed plan of this network should be developed and kept at a safe location.
- Library insurance should also cover the IT system of the library.
- Suitable measures should be taken to protect the library IT system from virus attack or hacking. Antivirus software or firewall must be installed.
- Monitoring of internet access by staff and readers. Measures should be taken which will prevent accessing of inappropriate sites.
- Use of redundant array of independent disks technology to capture on-line transaction activity.
- Taking suitable measures for protecting hardware from environmental damage, e.g. air-conditioning of the server room for protecting from dust, regular cleaning of the area, annual cleaning/servicing of the hardware.
- Providing training programmes for staff and readers on computer uses and ethics.
- Backup storage to be stored safely. One copy should be stored outside the library building premises.
- Data access security should be provided. Is data access provided through user name and password or IP based access? What rights are given to the reader in accessing the library data? e.g. readers should never be given right for editing of digital data.
- Appropriate physical security should be provided in the premises where computers and server are located, e.g. server room should be locked and should be protected from any type of damage likely to occur.
- Electrical cabling to be checked regularly to find any defect in the cables.

- Functionality of backups to be checked regularly, e.g. hardware and software used to create data may become outdated, so with new hardware and software backup data may be not accessible. Backup taken on CD/DVD may get corrupted. It may be required to migrate data to new platform to remain functional.
- If automatic backup software is installed, library staff must be trained for that and annual maintenance of software must be done by the library.
- A documentation procedure should be established to record any damage to hardware, software and digital data maintained by the library for insurance claim.
- Inventory of hardware and software available in the library must be maintained.

Being prepared to deal with a digital disaster should it occur in the library

To preserve and protect digital data and hardware and software from damage, every library must develop an Information Technology Disaster Recovery Plan or Technology Disaster Response Plan (Mallery, 2012). This will help not only in protection and recovery of data, hardware and software, but will also help in restoring library services at earliest:

> The ability to integrate or interoperate within and between storage systems is likely to make backup, disaster recovery and hardware migration services less risky across all storage systems and more economical for the University (Yale University Library, 2007).

Coping with recovery and restoration

Early efforts should be targeted at protecting and preserving the computer equipment. They should be identified and either protected from the elements or removed to a clean, dry environment, away from the disaster site.

While hardware and software are replaceable, data may not be if backups have not been properly maintained. Thus the first priority is to recover the data. If the data is on the internal hard disk an attempt should be made to recover as much of it as possible.

Water damage and fire damage need special attention.

If the hard disk has been under water for only a short time, the probability is that the head assembly has not been penetrated by the water. While the data recovery remains difficult, it can be done. If water has entered the small hole in the assembly head, speed is of essence. If the platters are accessed before the water dries, then there is still a chance of recovering the critical data on the drive. If the water does dry, it leaves behind minerals, dirt and other foreign materials throughout the drive, most importantly, the head assembly and platter(s). The chances of recovery at this point are less. It is important that the drive be kept wet. In requesting data recovery, it is important to seal the drive, as well as other media, in a container with a minimum of a damp sponge (Georges, 2004).

In case of fire, a risk to the head assembly is that the heat is so intense that the platters may melt. In this case, there is no hope of recovering the data. Even blackened drives can have undamaged head assemblies. The challenge in recovering data is to rebuild the electronics to access the data. The availability of data recovery services locally must be identified (Georges, 2004).

The damage to computer boards may be controlled by drying them quickly, possibly in an oven. It should not be done for hard disk as it can be disastrous (Georges, 2004).

Conclusion

Though there is awareness among librarians about the importance of protecting digital data, due to lack of knowledge, poor infrastructure, and absence of a digital data protection plan, digital data is in danger and may get damaged or destroyed in libraries if no actions are taken.

Librarians must be sensitized to the issues relating to data protection, and to recovery from disaster. As librarians are not IT specialists, training needs to be provided for digital data protection.

Libraries need to develop digital data protection policies. A disaster management plan should be prepared by all libraries, to cover all types of disasters. A section of this should be devoted to digital disasters.

The recommendations given above, while aimed at Indian libraries, would be applicable, at least basically, to all libraries.

References

Al-Badi, A.H., Ashrafi, R., Al-Majeeni, A.O. and Mayhew, P.J. (2009), "IT disaster recovery: Oman and cyclone Gonu lessons learned", *Information Management & Computer Security*, Vol. 17 No. 2, pp. 114-126, available at: www.emeraldinsight.com (accessed 23 April 2013).

Boss, R.W. (2002), "Disaster planning for computers and networks", available at: www.ala.org/ala/mgrps/divs/pla/tools/technotes/disasterplanning.cfm (accessed 15 June 2013).

Decˇman, M. and Vintar, M. (2013), "A possible solution for digital preservation of e-government: a centralised repository within a cloud computing framework", *Aslib Proceedings: New Information Perspectives*, Vol. 65 No. 4, pp. 406-424, available at: www.emeraldinsight.com (accessed 15 August 2014).

DiMattia, S.S. (2001), "Planning for continuity: special libraries close to the events of September 11 can serve as a model for the importance of being prepared", *Library Journal*, Vol. 126 No. 19, pp. 32-34, available at: www.libraryjournal.com/article/ CA180499.html (accessed 15 June 2013).

Disaster (def.) (1989), *In The Oxford English Dictionary*, 2nd ed., Vol. 4, Clarendon Press, Oxford.

Fox, R. (2006), "Vandals at the gates", *OCLC Systems & Services: International Digital Library Perspectives*, Vol. 22 No. 4, pp. 249-255, available at: www.emeraldinsight.com (accessed 24 May 2013).

Georges, J. (2004), "Skills development and management for disaster mitigation planning: the specific case of electronic equipment and digital data", *International Preservation News*, No. 34, pp. 12-14, available at: http://archive.ifla.org/VI/4/news/ipnn34.pdf (accessed 30 July 2013).

Grant, A. (2000), "Benighted! How the university library survived the Auckland power crisis", *Australian Academic & Research Libraries*, Vol. 31 No. 2, pp. 61-68, available at: http://dx.doi.org/10.1080/00048623.2000.10755116 (accessed 30 July 2013).

Hawkins, S.M., Yen, D.C. and Chou, D.C. (2000), "Disaster recovery planning: a strategy for data security", *Information Management & Computer Security*, Vol. 8 No. 5, pp. 222-229.

Illinois Institute of Technology (2012), "Paul V. Galvin Library: digital emergency preparedness and recovery plan", available at: http://library.iit.edu/disaster-plan/DigitalEmergencyPlan-current.pdf (accessed 30 July 2014).

International Federation of Red Crescent Societies (2002), *World Disasters Report: Focus on Reducing Risk: 2002*, Author, Geneva.

Jiazhen, L. and Daoling, Y. (2007), "Status of the preservation of digital resources in China: results of a survey", *Program: Electronic Library and Information Systems*, Vol. 41 No. 1, pp. 35-46, available at: www.emeraldinsight.com (accessed 30 July 2013).

Jiazhen, L. and Peng, D. (2009), "Long-term preservation of digital information in China: some problems and solutions", *Program: Electronic Library and Information Systems*, Vol. 43 No. 2, pp. 175-186, available at: www.emeraldinsight.com (accessed 30 July 2013).

Kahn, M.B. (2010), *Protecting Your Library's Digital Sources: The Essential Guide to Planning and Preservation*, ALA, Chicago, IL.

Kostagiolas, P., Araka, I., Theodorou, R. and Bokos, G. (2011), "Disaster management approaches for academic libraries: an issue not to be neglected in Greece", *Library Management*, Vol. 32 Nos 8/9, pp. 516-530, available at: www.emeraldinsight.com (accessed 30 July 2013).

Mallery, M. (2012), "Technology disaster response planning for libraries", available at: http://njlaconference.info/sites/njlaconference.info/files/technology_disaster_planning_for_libraries 2.pptx(pptpresentation) (accessed 20 August 2014).

Manaf, Z. and Ismail, A. (2010), "Malaysian cultural heritage at risk? A case study of digitisation projects", *Library Review*, Vol. 59 No. 2, pp. 107-116.

Oehlerts, B. and Liu, S. (2013), "Digital preservation strategies at Colorado State University libraries", *Library Management*, Vol. 34 Nos 1/2, pp. 83-95, available at: www.emeraldinsight.com (accessed 30 July 2013).

Raghavan, S., Sensarma, A.K. and Holland, G.J. (2009), "Chapter 7.5: warning strategies", in Holland, G.J. (Ed.), *Global Guide to Tropical Cyclone Forecasting*, Bureau of Meteorology, Melbourne, available at: http://cawcr.gov.au/bmrc/pubs/tcguide/ch7/ggch7.htm (accessed 30 July 2013).

Rinehart, A.K., Prud'homme, P.-A. and Huot, A.R. (2014), "Overwhelmed to action: digital preservation challenges at the under-resourced institution", *OCLC Systems & Services*, Vol. 30 No. 1, pp. 28-42, available at: www.emeraldinsight.com (accessed 25 August 2014).

Rothstein, P.J. (1998), "Disaster recovery in the line of fire", *Managing Office Technology*, Vol. 43 No. 4, pp. 26-30.

Sarantakos, S. (2005), *Social Research*, 3rd ed., Palgrave Macmillan, New York, NY.

Sidorko, P. and Lee, L. (2014), "JURA: a collaborative solution to Hong Kong academic libraries storage challenge", *Library Management*, Vol. 35 Nos 1/2, pp. 56-68, available at: www.emeraldinsight.com (accessed 20 August 2014).

Tennant, R. (2001), "Coping with disasters", *Library Journal*, Vol. 126 No. 19, pp. 26-28, available at: www.libraryjournal.com/article/CA180529.html (accessed 23 May 2013).

United Nations Development Programme and United Nations Disaster Relief Organization (1992), "An overview of disaster management", available at: http://iaemeuropa.terapad.com/resources/8959/assets/documents/UN%20DMTP%20-%20Overview%20of%20DM.pdf (accessed 15 April 2013).

Yale University Library (2007), "Policy for the digital preservation", available at: www.library.yale.edu/iac/DPC/revpolicy2-19-07.pdf (accessed 20 August 2014).

Yoon, C. and Kim, H. (2013), "Understanding computer security behavioral intention in the workplace: an empirical study of Korean firms", *Information Technology & People*, Vol. 26 No. 4, pp. 401-419, available at: www.emeraldinsight.com (accessed 20 August 2014).

Zainab, A.N., Chong, C.Y. and Chaw, L.T. (2013), "Moving a repository of scholarly content to a cloud", *Library Hi Tech*, Vol. 31 No. 2, pp. 201-215, available at: www.emeraldinsight.com (accessed 20 August 2014).

Zaveri, P. (2013), "Disaster management in libraries in India", unpublished doctoral dissertation, SNDT Women's University, Mumbai.

Further reading

Pasricha, P.S. (2006), "Disaster management: managing disasters", *One India One People*, Vol. 9 No. 10, pp. 8-11.

Stremple, R. and Martone, M.F. (2000), "Disasters come in all sizes", *InfoPro*, March, pp. 29-35, available at: www.rivercitydata.com/Pdfs/Documents/Disasters,Come In All Sizes.pdf (accessed 15 May 2013).

About the author

Dr Parul Zaveri is an Assistant Professor in Library and Information Science at SNDT Women's University, Mumbai. She has been teaching for more than 18 years and her areas of specialization are library management, digital libraries and reference and information sources and services. Dr Parul Zaveri can be contacted at: parulzaveri2004@yahoo.co.in