

## Information Security Measures of Libraries of Central Universities of Delhi : A Study

Vikas Singh and Madhusudhan Margam\*

*Department of Library and Information Science, University of Delhi, Delhi – 110 007, India*

*\*E-mail: mmadhusudhan@libinfosci.du.ac.in*

### ABSTRACT

The paper is to examine the information security measures, physical, organisational and technological in Jawahar Lal Nehru University (JNU), University of Delhi (DU) and Jamia Millia Islamia (JMI) in Delhi. The paper uses a mixed-method approach that combines both quantitative and qualitative analyses of information security measures with the help of a specially designed checklist. The findings of the study reveals that JNU scored 69.23 per cent highest information security features, followed by DU with 66.15 per cent, and JMI got the lowest total score with 63.07 per cent. The study has also revealed that all the university libraries under study have been lagging behind in physical security measures. It is hoped that the present study will help in improving the information security lacunas in libraries under study. The findings of the study will not only guide the university librarians to improve their Information security measures, but also open the floodgates for improvements of information security in fast changing technological world so that they can overcome the limitations being faced by librarians.

**Keywords:** Security measures; Physical security; technical security; organisational security; Delhi; India

### 1. INTRODUCTION

Library and information security is the method which has been used to conserve and preserve the integrity, availability and confidentiality of electronic information. Security control reduces the impact or probability of security threats and vulnerabilities to a level acceptable to the organisation. Information security is as important as it has ever been, but the challenges to determine the factors contributing to information insecurity prove to be of complex nature. In libraries, information systems (IS) are widely used to deliver services and collections to local and remote patrons. This is typically done in order to control access to the information in different ways, depending on its importance, its sensitivity, and its vulnerability to theft or misuse<sup>1</sup>. Moreover, connecting a library to the outside world via the Internet has changed the type of risks faced associated with and the controls used to secure the services the IS support<sup>2-5</sup>.

Information security management in the context of library management describes, controls that a library needs to implement to protect its information assets from all potential threats to ensure the confidentiality, integrity and availability of its information resources<sup>6</sup> and help to identify and reduce critical security risks and types of network attacks, for proper management of information security in digital libraries<sup>7</sup>. Libraries should be concerned about security and should spend considerable sums on preventing, detecting and resolving security breaches. In order, to reach desirable level of protection against threats and to provide the necessary mechanics to protect organisation's assets and knowledge, a vast variety of management approaches and methods have been

developed in the last decades. Libraries should review some of the plans, procedures, policies, some tools and methods that can be used to protect library system including Organisational, Physical and technological security. This paper gives an overview of current approaches in physical, organisational and technological security measures in select central university libraries in Delhi.

### 2. LITERATURE REVIEW

There are many articles and case studies available on this topic by various authors; some of the more relevant articles are reviewed. Information security is means and ways of protecting data from unauthorised access, change, misuse, loss and ensures its availability whenever required. At the beginning, information security was focused mainly on technical issues and the responsibility was left to technical experts<sup>8</sup>. University libraries face a number of security challenges with their collections (both print and non-print). Library collections constitute the bedrock for services provided to the community and serve as important assets to the library<sup>9</sup>. Uzuegbu & Caroline<sup>10</sup> developed a model named LISSAM (library information systems security assessment model), consistsof five components: information security policy, technological security foundation, administrative tools, methods, procedures and control and awareness creation. Ma<sup>11</sup>, *et al.* stressed upon the network security risks in digital medical libraries and their effective preventive measures, and pointed out the major flaws in their CD-ROM and full-text databases and their preventive measures.

RFID is considered to be the latest technology being used in libraries for self-checkout and check in, book identification, sorting and conveying of library books and for theft detection.

RFID system may be a comprehensive system that addresses both the security and materials tracking needs of a library. RFID technology saves money too and quickly gives a return on investment<sup>12</sup>. Samy<sup>13</sup>, *et al.* examine the hardware security threats that are damaging the physical components in an information system. On the other side, Gawde<sup>14</sup> presents the software security threats that are jeopardising the operating systems and related applications. Network security threats which are related to the network such as virus and hackers, whereas, data security threats is related to threats related to data, such as unauthorised access are discussed by various authors<sup>15-19</sup>.

Hagen<sup>20</sup>, *et al.* reveals implementation of organisational information security measures. Zhdanov<sup>21</sup> examines the information security solutions and policies which consist of three essays. The first two essays present theoretical models and the last essay used the data about attacks in network traffic in combination with graphical formalisms which is known as met graphs to derive information security policy rules. It also provides the practitioners, newcomer with a systematic but intuitive way to analyse information security policies whereas, good design of a library should integrate security for the protection of its collections, building and its occupants. The main focus is to give an environment that balances both safety and comfort. Carey<sup>22</sup> explain the passive security measures such as transparency, openness, visibility, and building organisation are key to the creation of a safe environment. Ohno<sup>23</sup> re-investigated the security measures suffered from natural disasters such as earthquakes, torrential rains and heavy snowfall. In this article, he reports some of his attempts to improve the situation and suggests the type of system to purchase including computers in place, the security needed to protect the past and present campus security issues. Butters<sup>24</sup> discuss the threats of RFID technology in libraries and to probe their technical feasibility and what sort of action should be taken by libraries to take the edge off the risk that actually exists.

Ismail & Zainab<sup>25</sup> proposes an instrument to assess the current information systems security status in libraries. Akor<sup>26</sup> analysis showed that the university library books are stolen and mutilated due to inadequate library materials, financial constraint and selfishness on the part of library users. The study recommends that university management should provide adequate library materials to meet the information needs of their users. Hanus<sup>27</sup> examines the theory by proposing and validating a universal definition of security awareness. It provides practitioners with an instrument to examine awareness in a plethora of settings and design customised security training activities. Olijnyk<sup>28</sup> adds to the accumulated wealth of knowledge on the science of scholarly domains by shedding light on the nature of speciality development. Silic & Back<sup>29</sup> gives a critical review and future directions of research in information security. Kim<sup>30</sup> reveals in his paper regarding the information security awareness among the college students. Newby<sup>31</sup> gives a description of information security for libraries. Ellern<sup>32</sup> have looked at the state of authentication practices within a specific region (i.e., all the academic libraries in North Carolina) in an attempt to create a profile of those libraries that choose to

authenticate or not. Jackson<sup>33</sup> describes the tips for creating awareness and best practices for cyber security for information professionals.

### 3. OBJECTIVES

The objectives of the study are:

- (i) To study the different information security measures with regard to Physical, Organisational and Technological in university libraries under study;
- (ii) To compare the different information security measures in studied libraries and rank them based on various features, and
- (iii) To provide suggestions for improve information security measures in studied libraries.

The scope of the study is confined to three central universities in Delhi, i.e., University of Delhi (DU), Jawaharlal Nehru University (JNU), and Jamia Millia Islamia University (JMI). The study aims to evaluate the information security measures in studied libraries. Table 1 presents the list of Central University libraries in Delhi with their establishment and universal resource locators (URLs).

A structured checklist was designed keeping in view of the stated objectives and literature available so as to know various qualitative and quantitative information security features. The Checklist comprises of 77 questions, categorised as two main parts, preceded by a rating Table, viz. Part-I: *Qualitative analysis* (12 descriptive questions) and Part-II: *Quantitative analysis* (65 questions). Each part of the checklist contains a set of related questions and the responses of the each section are presented in respective tables.

**Table 1. Central universities library websites and their year of Establishment**

University Library	URL of the library
Central Library, University of Delhi (DU) <sup>34</sup>	<a href="http://crl.du.ac.in">http://crl.du.ac.in</a>
Dr. B.R. Ambedkar Central Library, Jawaharlal Nehru University (JNU) <sup>35</sup>	<a href="http://www.jnu.ac.in/Library/Intro.htm">http://www.jnu.ac.in/Library/Intro.htm</a>
Dr. Zakir Husain Library, Jamia Millia Islamia (JMI) University <sup>36</sup>	<a href="http://jmi.ac.in/zhlbrary">http://jmi.ac.in/zhlbrary</a>

### 4. DATA ANALYSIS AND INTERPRETATION

The data analysis took place during 20 July 2016 to 21 August 2016. The qualitative and quantitative responses were received from evaluation checklists. Each time a cell (i.e., specific feature in the checklist) was checked, one point was assigned to the respective feature marked “√” (yes) and no point for marked “x” (no) in the study. The score for a system is the total number of cells checked for that security system. Each part has a set of related questions and the responses of the each part and their sub parts were analysed with the help of tables followed by interpretation of data.

#### 4.1 Qualitative Analysis

The qualitative analysis contain various essential features such as, software, anti-spyware software, cleanup software, user identification and authentication, firewall, antivirus software,

server location, internal and remote computer systems, security of network equipment's and emergency power sources. The qualitative analysis of the checklist having Twelve (12) features pertaining to select security systems, which is serving in the form of a recording device for descriptive data.

Table 2 reveals that 100 per cent university libraries are using Library automation software of which JNU is using Virtua, JMI is using Libsys and DU is using Troodon software. Both JNU and JMI Libraries are using Quick Heal antivirus software to detect and remove any spyware threats whereas DU is using Symantec Antivirus to detect and remove any spyware threats. Studied Libraries are using CC Cleaner software to erase files or settings left behind by a user and using identification and authentication at computer network, whereas, JNU and JMI has library network. Further, JNU also uses user identification and authentication at laptops, screen savers, and at remote access.

JNU and DU uses application of firewall and DU also uses hotspot for mobile laptops that connect to the library's LAN, whereas, no such application is available in JMI. All the studied libraries are using antivirus software to secure library server, JNU is using Symantec Endpoint protection and Quick Heal, whereas, JMI is using only Quick Heal and DU is using Symantec Endpoint protection. All the studied Library servers are placed in a secure location i.e., separate and locked room, whereas JNU and DU is also using environmental control area for this purpose. JNU and DU are using single sign-on system to control data access to the library internal and remote computer systems which is not present in JMI. For the security of network equipment's security, cables, locked cable trays, metal cages or

anchoring devices is being used by JNU, whereas, DU is using metal cages or anchoring devices for this purpose but no such devices are being used in JMI.

For emergency power sources and alternative communication lines all the studied libraries are using telephone lines, generators/ inverters, UPS, etc. JNU and DU both are using system recovery to rebuild, repair the library computers systems after disaster or crash in selected institutional libraries, but it is not present in JMI. All the studied libraries are using Firewall web filtering software to prevent access to inappropriate materials or sites and as well as web filtering software.

**4.2 Quantitative Analysis**

The quantitative part of the checklist contains 65 dichotomous questions relating to:

- (i) Organisational security
- (ii) Physical security, and
- (iii) Technological security.

Detailed analysis of each category is presented in the presiding sections:

*4.2.1 Organisational Security*

An organisational security measure is done by calculating the sum value for the presence of procedures, controls, security policy, administrative tools and awareness creation. This section having 14 questions related to different aspects of organisational security (Table 3).

Table 3 reveals that JNU and DU libraries are having written library & information science security policy, whereas

**Table 2. Qualitative aspects of security systems**

Qualitative aspect of security systems	JNU	JMI	DU
Library Management Software	Virtua	LibSys	Troodon
To detect, remove any spyware threats by use of Anti-spyware software	Quick Heal Antivirus	Quick Heal Antivirus	Symantec Antivirus
Cleanup software for erasing files or settings left behind by a user	CC Cleaner	CC Cleaner	CC Cleaner
Identification and authentication required for logging	Workstations, Laptops, Screen savers, Library Network, Computer Network, Remote Access	Workstations, Library Network, Computer Network	Computer Network
Use of firewall for mobile laptops that connect to the library's LAN	Firewall System	--	Firewall System and Hotspot
Antivirus software to secure library server	Symantec Endpoint protection, Quick Heal	Quick Heal	Symantec Endpoint protection
Server Location	Separate and locked Room, Environmental Control Area	Separate Room	Separate and locked Room, Environmental Control Area
Data Access Control	Single Sign-on System		Single Sign-on System
Network Security equipment's	Locked Cable Trays, Security Cables, Metal cages/ anchoring devices		Metal cages or anchoring devices
Use of alternative communication lines and emergency power sources	Telephone Lines, Generators/ Inverters, UPS	Generators/ Inverters	Generators/ Inverters
System recovery to rebuild, repair the library computers systems	Dell Recovery System		Available*
Web filtering software	Firewall	Firewall	Firewall

Note= JNU- Jawaharlal Nehru University, JMI- Jamia Millia Islamia, DU -University of Delhi.

JMI is not having any such policy. Further, data classification, retention and destruction policies for library data or materials that contain sensitive information are present in JNU only. All the studied libraries are identified management policies for library and information system, user registration, password management, library hardware security, data security, software security and they allow use of wireless devices in their library such as laptops and hand devices except in DU. Further, all the studied libraries having policy on sharing, storing and transmitting of library data via external networks or third party systems. JNU and DU have the procedure for reviewing the current information security policy and they both have security administrator and have contingency disaster plan/ risk management policy for dealing with natural and man made disasters, whereas these are not existing in JMI.

Interestingly, 100 per cent staff and patrons in studied libraries at various levels are made aware of their responsibilities with regards to protecting the information systems security and also provide Library and information security training and orientation programs to their staff. Further, JNU and DU libraries organise program/workshop for staff/ patrons regarding information security and well defined structured information available in their library websites.

#### 4.2.2 Physical Security

Physical security indicates that unauthorised access into the library building, leaking and theft or vandalism threats

**Table 3. Organisational security**

Organisational Security Features	Institution		
	JNU	JMI	DU
Library & information science security policy	✓	X	✓
Classification of data, retention , destruction policies for sensitive information	✓	X	X
Identified management policies for user registration and password management	✓	✓	✓
Written policy regarding library hardware security	✓	✓	✓
Written policy regarding data security	✓	✓	✓
Written policy regarding software security	✓	✓	✓
Use of wireless devices in library such as laptops and hand phones.	✓	✓	X
Policy on storing, sharing and transmitting of library data via external networks or contractors systems.	✓	✓	✓
Procedure for reviewing security policy	✓	X	✓
Security administrator	✓	X	✓
Contingency disaster plan/ risk management policy	✓	X	✓
All staff aware of their responsibilities regarding security	✓	✓	✓
Training and education programs for staff	✓	✓	✓
Organise program/workshop for staff/patrons	✓	X	✓
Total Score (maximum 14)	✓	08	12

Note= '✓' = Yes; 'X' = No.

in participating libraries. This section is having 24 features related to physical security features existing in studied libraries (Table 4).

Table 4 reveals that all the selected libraries under study uses air conditioning to stabilise the humidity and temperature in the library building, whereas only JNU Library uses earthquake early warning system to alert library staff and patrons prior to damaging ground shaking but no studied library found to be using any kind flood detector to provide an early warning of developing floods in their libraries. Only JNU and DU Library Systems are using lighting protectors and surge protectors to protect any valuable machines or equipment's from lighting strikes, voltage spikes and surges, whereas, 100 per cent institutions keep security guards to monitor people entering and leaving the library buildings and sites, but only JMI uses

**Table 4. Physical security**

Physical Security Features	Institution		
	JNU	JMI	DU
Air conditionings to stabilise the temperature and humidity	✓	✓	✓
Earthquake early warning system	✓	X	X
Flood detector an early warning system	✓	X	X
Lighting protectors and surge protectors	✓	X	✓
Security guards to monitor people	✓	✓	✓
Automatic Sprinkler System (fighting against intense fires)	X	✓	X
Smoke Detector	X	✓	X
Fire extinguishers	✓	✓	✓
Fireproof Installation the building and areas	✓	✓	X
<b>User identification and authentication entrances and exits</b>			
Magnetic stripe swipe cards	✓	X	X
Electronic Locks	X	X	X
Proximity cards	X	X	X
Wireless gates	X	X	X
Biometrics System	X	X	X
<b>Window security</b>			
Locks	✓	✓	✓
Guards	X	✓	✓
Grillers	✓	✓	✓
Bars	X	✓	✓
Screens	✓	✓	✓
Films	X	✓	✓
<b>Door protection security</b>			
Cylindrical locks	✓	X	X
Deadbolts	X	X	X
Mortise locks	✓	X	X
Normal Door Locks	X	✓	X
Total Score (maximum 24)	12	13	10

Note= '✓' = Yes; 'X' = No.

automatic sprinkler system (fighting against intense fires) and smoke detector in the library building and areas, because it was built newly.

100 per cent studied libraries are using Fire extinguishers in their library building and nearby areas. On the other hand, JNU and JMI are using fireproof installation in the library building and surrounding areas. In the user identification and authentication entrances and exits segment only, JNU user uses magnetic stripe swipe cards. Interestingly, no studied Library uses electronic locks, proximity cards, wireless gates or biometrics system for this purpose (biometrics system being used for staff attendance). Window security (lock, grillers, screens) and bars are available in all studied libraries but films are available only in JMI and DU. Door protection security i.e., cylindrical locks, mortise locks are available in only JNU, whereas deadbolts facility is not available in any of the studied library. Further, normal door locks are present in JMI.

4.2.3 Technological Security

The Technological security refers to the security of library software, hardware, network security, server security, data security, workstations security and electronic security systems such as RFID, Fire alarms, Burglary protection and barcode, etc. This is the last part of the checklist and having highest number of features, i.e., 27 features related to technological security of the studied libraries (Table 5).

Table 5 reveals that all studied libraries uses technological security features except desktop security software for disable certain features of workstations, tests and automatic debugging to remove any defects from hardware components or new software, virus protection and security programs/ software(s) that installed for web browser and email programs and also system recovery to repair, rebuild the library computers systems.

Interestingly, in the context of electronic security system none of the studied libraries are using RFID system to protect library materials, motion/sensor detectors and smart cards. Barcode technology was used for their routine work, and CCTV was to safeguard their materials were common in all studied libraries, but, only Delhi University was using Biometrics system for staff attendance. Furthermore, JNU and JMI Libraries are using Fire alarm. Moreover, JMI and DU have installed CCTV cameras in Reading room, but, JNU and DU have done it in stack rooms. JMI and Delhi University has installed CCTV cameras in corridors and server area computer labs which were sensitive and expensive. Surprisingly, all the studied libraries are using web filtering software to prevent access to inappropriate materials or sites.

5. TOTAL SCORE OF INFORMATION SECURITY MEASURES

The total score of study information security measures (ISM) is presented in Table 6 on the basis of previous respective Tables 3, 4 and 5 (Quantitative analysis). A quantitative five point rating scale was designed based on intensity scale suggested by Taylor-Powell<sup>37</sup> to range from ‘very high’ to ‘very low’ to rank the each individual information security measure and to aid in

Table 5. Technological security

Technological security features	Institution		
	JNU	JMI	DU
Authentication for software	√	√	√
Authorisation for software	√	√	√
Privacy for software	√	X	√
Workstation security from threats and viruses	√	√	√
Desktop security software for disable certain features of workstations	√	√	X
Tests and automatic debugging to remove any defects from hardware components or new software	√	√	X
Virus protection and security programs/ software(s) that installed for web browser and Email programs	X	√	√
System recovery to repair, rebuild the library computers systems	√	X	√
Desktop security software and antivirus software to receive regular updates	√	√	√
Wi-fi connection	√	√	√
Network identification and wireless intrusion detection systems	√	√	√
Server protection	√	√	√
Anti-virus software on servers and antivirus definition files are kept up-to-date	√	√	√
Regular backups of data	√	√	√
<b>Electronic security system</b>			
RFID	X	X	X
Barcode	√	√	√
CCTV	√	√	√
Biometrics	X	X	√
Fire Alarms	√	√	X
Motion/sensor detectors	X	X	X
Smart Cards	X	X	X
<b>CCTV cameras</b>			
Reading room	X	√	√
Stack rooms	√	X	√
Corridors	X	√	√
Computer labs	√	√	√
Server areas	X	√	√
Web filtering software to prevent from inappropriate materials or sites	√	√	√
Total Score (maximum 27)	19	20	21

Note= ‘√’ = Yes; ‘X’ = No

distinguish quality under study. The five-point rating scale was fixed equally based on the maximum quantitative score of 65 points. Range (Score): 53-65 – Very High; 40-52 = High; 27-39 = Medium; 14-26 = Low; and 01-13 = Very Low.

Table 6 presents the list of all three aspects of security measures in studied libraries. Total features existing among the three security measures amounting for 129 out of 195, of

which, technical security features tops with 60, followed by physical security features (35) and with slight difference with organisational security features (34).

A cursory glance at the Table 6 reveals that out of three studied universities, none of the studied university had ranked 'Very High'. All the studied libraries were ranked with 'High', of which JNU got the highest total score of 45 out of 65 (69.23 per cent), followed by DU with 43 score (66.15 per cent). Interestingly, JMI got the lowest total score with 41 (63.07 per cent).

**Table 6. Total score of ISM**

Information security measures and maximum Score	JNU	DU	JMI	Total features
Organisational security (maximum 14)	14	12	08	34/42
Physical security (maximum 24)	12	10	13	35/72
Technical security (maximum 27)	19	21	20	60/81
Total score (maximum 65)	45	43	41	129/195
Rank	High	High	High	

## 6. SUGGESTIONS

The study proposes the following suggestions for effective implementation of information security measures in studied libraries:

- (i) Use of firewall for mobile devices that connect to the library's LAN is very essential which is being used by JNU and DU only which may be used by JMI to caters the need of present day readers.
- (ii) Network security equipment's such as: Locked cable trays, Security cables, metal cages/ anchoring devices are essential equipment they should be used in JMI Library for better security purposes.
- (iii) System recovery to rebuild, repair the library computers systems are integral part of any network security. Only JNU uses Dell Recovery System, whereas, otherstudied libraries should use some kind of network security system.
- (iv) As far as Organisational security is concerned, JMI lacks in most of the features such as LIS security policy, classification of data, retention, destruction policies for sensitive information, written policy regarding data security and software security, procedure for reviewing security policy, contingency disaster plan/ risk management policy which must be focused by JMI.
- (v) University of Delhi must focus on Physical security aspects like, Air conditioning to stabilise the temperature and humidity, earthquake early warning system, flood detector an early warning system, smoke detector, fire extinguishers, etc.

## 7. CONCLUSIONS

This study provides a quantitative and qualitative approach

that investigated the implementation status of information security measures through the opinions of respondents. The study also pointed that information security is to be effective; libraries need to incorporate technical measures as well as information security policies, security procedures and awareness creation activities in their security programmes. The findings of the study, Jawaharlal Nehru scored highest followed by University of Delhi, and Jamia Millia Islamia. Furthermore, it was also found that all the institutions selected for study have been lagging in physical security measures more and they have to strengthen this area. It is hoped that the present study will be boon for developing counties give an idea to the Librarians and library professionals in forming Library and information security policy for their libraries. The robustness of this instrument need to be further tested and this will carried out in the second phase of this Study.

## REFERENCES

1. Rhodes-Ousley, M. *Information security*. Ed. 2nd. McGrawHill, New York, 2013, 3. <https://www.mheducation.com/highered/product/information-security-complete-reference-second-edition-rhodes-ousley/0071784357.html>.(Accessed on 18 March, 2017).
2. Gupta, M. & Sharman, R. Social and human elements of information security: Emerging trends and countermeasures. Hershey, 2008, PA: IGI Global.
3. Guttman, B. & Roback, E. An introduction to computer security: The NIST Handbook. NIST special publication 800- 1. Washington, DC: US National Institute of Standards and Technology, 1995. <http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf> (Accessed on 10 September, 2016).
4. Scarfone, K.; Souppaya. M. & Cody, A. Technical guide to information security testing and assessment. Technical Report Special Publication 800-11. Washington, DC: US Department of Commerce, National Institute of Standards and Technology, 2008. <http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf> (Accessed on 21 September, 2016).
5. Westby, J.R. & Allen, J.H. Governing for enterprise security (GES) implementation guide.CMU/SEI-2007-TN-020.Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2007. <http://www.cert.org/archive/pdf/07tn020.pdf> (Accessed on 21 September, 2016).
6. Ismail, R.B. Assessing information security management in Malaysian academic libraries. Faculty of Computer science and information technology, University of Malaya, Kaula Lumpur, PhD thesis, 2012, 268.
7. Ravi, B. Information security in digital libraries. *In* Library Security Management in Digital Era: Proceedings of the National Conference NCLMS-2011, February 4<sup>th</sup>-5<sup>th</sup>, 35-43.
8. Von, S. B. Information security- the third wave? *Computers and Security*, 2000, **19**, 615-620. [http://www.tut.fi/units/tuta/tita/2006-2007/TITA-300/the\\_third\\_wave](http://www.tut.fi/units/tuta/tita/2006-2007/TITA-300/the_third_wave). (Accessed on 11 September, 2016).

9. Maidabino, A.A. & Zainab, A.N. Collection security management at university libraries: Assessment of its implementation status. *Malaysian J. Lib. Inf. Sci.*, 2011, **16** (1), 15-33.
10. Uzuegbu, C.P. & Caroline, A.O. Security practices in Nigerian university libraries. *PNLA Quar.*, 2013, **77**(2), 18-27. <https://ajba.um.edu.my/index.php/MJLIS/article/view/6675> (Accessed on 25 March, 2017).
11. Ma Jun-tao, D.; Huang, Qiu-sheng, & Wen, S X. Network Security risks in digital medical libraries and their preventive measures. *Chinese J. Med. Lib. Inf. Sci.*, 2010, **19** (6), 60-1.
12. Madhusudhan, M. & Gupta, P. Use of RFID technology by students in Indian Institute of Technology, Delhi and Indian Law Institute, Delhi: A survey. *World Dig. Libraries*, 2014, **7**(2), 145-156.
13. Samy, G.N.; Rabiah, A. & Zuraini, I. Security threats in healthcare information systems: A preliminary study. In Fifth International Conference on Information Assurance and Security. *IEEE Comp. Society*, 2009 (18-20 August).
14. Gawde, V. Information systems misuse - threats & countermeasures, *Infosecwriters*, 2004 [http://infosecwriters.com/text\\_resources/pdf/information\\_systems\\_misuse.pdf](http://infosecwriters.com/text_resources/pdf/information_systems_misuse.pdf).> (Accessed on December 10, 2016).
15. Williams, R.L. Computer and network security in small libraries: A guide for planning. Texas State Library Archive Com, 2001. <http://www.tsl.state.tx.us/ld/pubs/compsecurity/> (Accessed on 21 September, 2016).
16. Farahmand, F.; Navathe, S.B.; Sharp, G.P. & Enslow, P.H. Assessing damages of information security incidents and selecting control measures: A case study approach. In Workshop on the Economics of Information Security, 2005. <http://infoecon.net/workshop/pdf/39.pdf> (Accessed on 11 November, 2016).
17. Eisenberg, J. & Lawthers, C. Library computer and network security. *Infopeople*, 2005. <http://www.infopeople.org/resources/security> (Accessed on 1 November, 2016).
18. Mell, P.; Kent, K. & Nusbaum, J. Guide to malware incident prevention and handling. National Institute of Standards and Technology, Special Publication 800-83, Gaithersburg, MD, U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology, 2005. <http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf> (Accessed on 21 September, 2016).
19. Yeh, Q. & Chang A.J. Threats and countermeasures for information system security: A cross-industry study. *Inf. Mgt.*, 2007, **44**, 480-491. <https://pdfs.semanticscholar.org/814b/46a816bbb07ab82139df257e9adaca3ee49f.pdf> (Accessed on 25 May 2017)
20. Hagen, J.M.; Eirik, A. & Jan, H. Implementation and effectiveness of organizational information security measures. *Inf. Mgt. Comp. Sec.*, 2008, **16**(4), 377-97. doi: 10.1108/09685220810908796>
21. Zhdanov, D. Information security in organizations: Drivers, policies and compliance incentives. University of Minnesota, 2007.
22. Carey, J. Library security by design. *Lib. Arch. Sec.*, 2008, **21**(2), 129-40.
23. Ohno, F. Current state of security at the Niigata university medical and dental library. *J. Japan Med. Lib. Assn.*, 2008, **55**(1), 30-3.
24. Butters, A. RFID systems, standards and privacy within libraries. *The Elect. Lib.*, 2007, **25** (4), 430-9. doi: 10.1108/02640470710779844
25. Ismail, R. & Zainab, A.N. Information systems security in special and public libraries: An assessment of status. *Malaysian J. Lib. Inf. Sci.*, 2011, **16**(2), 45-62. <https://arxiv.org/ftp/arxiv/papers/1301/1301.5386.pdf> (Accessed on 20 October, 2017).
26. Akor, P.U. Security management for prevention of book thefts in university libraries. A case study of Benue state university library, Nigeria. *Lib. Phil. Prac.*, 2013. <http://digitalcommons.unl.edu/Libphilprac/995> (Accessed on 25 November, 2016).
27. Hanus, B. T. The impact of information security awareness on compliance with information security policies: A phishing perspective, 2014. <http://search.proquest.com/docview/1719103457?accountid=10461> (Accessed on 20 December, 2016).
28. Olijnyk, N.V. Information security: A scientometric study of the profile, structure, and dynamics of an emerging scholarly speciality, 2014. <http://search.proquest.com/docview/1530479755?accountid=10461> (Accessed on 21 September, 2016).
29. Silic, M. & Back, A. Information security: critical review and future directions of research. *Inf. Mgt. Comp. Sec.*, 2014, **23**(3), 279-308. doi: 10.1108/IMCS-05-2013-0041
30. Kim, E. Recommendations for information security awareness training for college students. *Inf. Mgt. Comp. Sec.*, 2014, **22**(1), 115-126. doi: 10.1108/IMCS-01-2013-0005
31. Newby, G.B. Information security for libraries, 2014. <https://www.petascale.org/papers/library-security.pdf> (Accessed on 5 October, 2016).
32. Ellern, G.; Hitch, R. & Stoffan, M.A. User authentication in the public area of academic libraries in north Carolina. *Inf. Tech. Libr.*, 2015, **34**(2), 103-132. doi: 10.6017/ital.v34i2.5770
33. Jackson, D.W. Cyber security: Best practices for information professionals. *AALL Spectrum*, 2016, 12-16.
34. Central Library, University of Delhi (DU). <http://crl.du.ac.in> (Accessed on 1 November, 2016).
35. Dr. B.R. Ambedkar Central Library, Jawaharlal Nehru University (JNU) <http://www.jnu.ac.in/Library/Intro.htm> (Accessed on 10 November, 2016).
36. Dr. Zakir Husain Library, Jamia Millia Islamia (JMI) University. <http://jmi.ac.in/zlibrary> (Accessed on 10 November, 2016).
37. Taylor-Powell, Ellen. Ways to word answer choices in questionnaires, Program Development and Evaluation, University of Wisconsin System, 2008. <https://www.scribd.com/document/338993195/English-Multiple-Choice-Likert-Answers> (Accessed on 27 October, 2017).

## CONTRIBUTORS

**Mr Vikas Singh** is currently working in the Shri Ram College of Commerce, University of Delhi, New Delhi. He obtained his MLISc and MPhil in Library and Information Science from the University of Delhi and Post Graduate Diploma in Library Networking from Indira Gandhi National Open University, New Delhi. He presented several papers in Conference/Seminar and published in Journals. His specialised fields are Library management software and library security measures.

**Dr M. Madhusudhan** is currently working as an Associate Professor in the Department of Library and Information Science, University of Delhi. Under his supervision 17 PhDs were awarded. He has published three books, more than 60 research articles and 25 chapters. His areas of interest are evaluation of websites and web-OPACs, ICT in libraries, social networking sites, e-resources, mobile-based library services, etc.