Open Source Softwares in Libraries: Threats and Challenges

Anjaneya Reddy N M
Research Scholar
Department of Library & Information Science
Bangalore University, Bengaluru – 560 056
e-mail: areddy.ragini@gmail.com

Dr. Lalitha Aswath
Professor
Department of Library & Information Science
Bangalore University, Bengaluru – 560 056
e-mail: drlalitha.aswath@gmail.com

ABSTRACT

Continuous dependence on open source software for Library operations has increased the necessity of managerial skills for managing risks while using the open source software. Here an attempt has been made to identify the risk factors, security measures and strategies for using open source software to manage the library operations effectively. Libraries have to create suitable and adequate environment to deal with risks during selection, implementation and use thereafter.

Keywords: Risk Management, Open source software, Library Management, Strategies, Security Measures.

1. Introduction

Information professionals are working in very complex but interesting times. They provide effective service by using open and hidden digital resources on the internet which is a challenging task for the library professionals. The modern libraries are always innovative and providing a variety of new services to their users with the help of ICT applications. Currently many computer applications are open source and available for libraries to provide wide range of services such as library automation, library website management, knowledge management, digital library management etc. These open-source softwares have become increasingly popular in library environment, and large numbers of libraries are migrating to open-source software movement.

There are many discrete open source softwares and applications are available for automation of libraries and promotion of services. Library softwares such as Dspace, GSDL, e-Prints, Koha, Zoomla, ABCD, Drupal, NewGenlib and many more are available for library management. Large number of open source softwares are coming-up to assist the libraries and librarians in providing efficient, effective and continuous information service to their clients.

2. Open Source Softwares and Risk Management

2.1 Open Source Software

Open source software[i]refers to both a model of software development and an ideology of intellectual property. The word open indicates that the program's source code is freely accessible to anyone and also can be modified and redistributed without paying a royalty or licensing fee, i.e. ‘Copy left’. Open source software is often developed in public domain.

Open source software, computer software whose source code is put into the public domain, subject to the restriction that any derived software also includes the source code and be put into the public domain.

Open source software[ii] is software which is licensed to guarantee free access to the programming behind the pre-compiled binary, otherwise called the ‘source code’. This allows the user to install the software on a new platform without an additional purchase, to get support (or create a support mechanism) for a product whose creator no longer supports it. Those who are technically inclined can fix bugs themselves rather than waiting for someone else to do so. Generally there is a distribution mechanism, such as anonymous ftp, which allows one to obtain the source code, as well as pre-compiled binaries in some cases. There are also mechanisms for which one may pay a fee to obtain the software as well, such as on a CD-ROM or DVD, which may also include some technical support. A variety of licenses are used to ensure that the source code will remain available, wherever the code is actually used.

Open source software means not only access to the source code, it should also meet the distribution and redistribution terms of open source software criteria[iii] which are as follows;

1. Free Redistribution

The license shall not restrict any party from selling or giving away the software as a component of an aggregate software distribution containing programs from several different sources. The license shall not require a royalty or other fee for such sale.

2. Source Code

The program must include source code, and must allow distribution in source code as well as compiled form.

3. Derived Works

The license must allow modifications and derived works, and must allow them to be distributed under the same terms as the license of the original software.

4. Integrity of the Author's Source Code

The license may restrict source-code from being distributed in modified form only if the license allows the distribution of "patch files" with the source code for the purpose of modifying the program at build time. The license must explicitly permit distribution of software built from modified source code. The license may require derived works to carry a different name or version number from the original software.

5. No Discrimination against Persons or Groups

The license must not discriminate against any person or group of persons.

6. No Discrimination against Fields of Endeavor

The license must not restrict anyone from making use of the program in a specific field of endeavor. For example, it may not restrict the program from being used in a business, or from being used for genetic research.

7. Distribution of License

The rights attached to the program must apply to all to whom the program is redistributed without the need for execution of an additional license by those parties.

8. License Must Not Be Specific to a Product

The rights attached to the program must not depend on the program's being part of a particular software distribution. If the program is extracted from that distribution and used or distributed within the terms of the program's license, all parties to whom the program is redistributed should have the same rights as those that are granted in conjunction with the original software distribution.

9. License Must Not Restrict Other Software

The license must not place restrictions on other software that is distributed along with the licensed software. For example, the license must not insist that all other programs distributed on the same medium must be open-source software.

10. License Must Be Technology-Neutral

No provision of the license may be predicated on any individual technology or style of interface.

2.2 Open Source Software - historical perspective

History of open source is closely runs with the growth and development of software itself. Richard Stallman, GNU, and Free software foundation is responsible for laying much of the groundwork for what has become the open source movement. During 1970s and early 1980s, he was working with MIT as a programmer and developed an operation software system where they use to share any of it with anybody. And anybody was welcome to see, take away, use and modify it. There was no copyright notice on these programs. To support the development of GNU (General Public License), Stallman founded the Free Software Foundation in the year 1985 and in 1989 the first version of GNU was released by him.

Since 1985many OSS initiatives have been made resulting in establishment of many associations or foundations to promote OSS. Some of the associations[iv]founded are;

a) Free Software Foundation - 1985
b) Python Software Foundation - 1990
c) Open Source Initiative (OSI) - 1998
d) Mozilla Foundation - 1998
e) Apache Software Foundation -1999
f) Drupal Association - 1999

g) Open Source Software Institute - 2000
h) Eclipse Foundation - 2001
i) Creative Commons - 2001
j) Open Source Matters, Inc. (Joomla)- 2005
k) New Zealand Open Source Society (Foss) - 2005
l) GNOME Foundation - 2005
m) Linux Foundation - 2007
n) Apereo Foundation - 2012

2.3 Purpose of Open Source Software

- To promote creative development of software
- To help those who can't afford proprietary software, can choose open source programs
- To customize the software as per their library needs
- To make new version freely available
- To establish community discussion forums which are freely available for help
- To promote computer literacy among professionals
- To make it easy to migrate to any other software

2.4 Risk Management

Risk is a probable uncertainty in success or goal reaching. Risk can also be defined as 'hazard, a chance of bad consequences, loss or exposure to mischance'. Any action or an event that affect negatively on an organization to achieve its goals successfully is called risk. A systematic process of managing risk is called Risk management. (Oxford English Dictionary)

The characteristics of risks are;

a) Uncertainty - the risk mayor may not happen
b) Loss-the risk becomes a reality and unwanted consequences or losses occur

Risk can bring in consequences in terms of economic performance and professional reputation, as well as environmental safety and societal outcomes in an organizational management. Effective risk management is inevitable for better management in an uncertain environment. (ISO)

Risk management is relatively a recent corporate concept function. During the recent years it has been in operation in all fields. Risk management is an organized method or process for identifying and measuring risk and for selecting, developing, and implementing options for the handling of risk factors associated with any project or situation. Risk management includes planning, identification and analysis of risks, continuous risk tracking and reassessment, early implementation of corrective actions, communication, documentation, and coordination.

2.5 Principles of Risk Management

2.6 The International Organization for Standardization[v] (ISO) categorized the following principles of risk management;

1. Create value

2. Be an integral part of organizational processes
3. Be part of decision making process
4. Explicitly address uncertainty and assumptions
5. Be systematic and structured
6. Be based on the best available information
7. Be tailored
8. Take human factors into account
9. Be transparent and inclusive
10. Be dynamic, interactive and responsive to change
11. Be capable of continual improvement and enhancement
12. Be continually or periodically re-assessed

3. Risk Factors in OSS

Any project implementation through open source software may lead to many risks. Especially for librarians it's a challenging task where they need to balance the manpower and the money. The risk factors[vi]that may affect heavily on execution of open source software in the libraries are;

3.1 Data security: Protecting data from unauthorized access or manipulation of data in the database. The open source softwares are available freely to all those who wants to use. It is highly difficult to have control over the data and unauthorized persons may hack the data easily in the open source software scenario. The code of open source software is created and uploaded on the internet by the program developers and chances are open to modify or corrupt the code by unauthorized persons. For instance many libraries are using 'Koha', library automation software for its routine operations and the same is being hosted on cloud computing'. The cloud computing[vii] might have helped to take away the problem of setting up their own hardware and managing it, but it could also take away your data, with so many free online office suites and online storage service providers out on the cloud, it's very easy to take out data under the guise of accessing it from anywhere.

3.2 Lack of Skills: Skilled persons are required to execute and implement the open source software in a proper manner. Lack of software technologyskills[viii]among library professionals is another major risk to implement open source software in the library environment. Dependence on IT experts or skilled persons enhances the library expenditure and defeats the purpose of OSS movements.

3.3 Training: Adequate training is a prerequisite for the success of open source software movement among working professionals. It is also one of the risk factors that how to train the library staff on operational modules of open source software. It includesupdation of new versions too. Continuous training supportis required to cope-up with the new versions and technology.

3.4 Up-gradation: To upgrade to the new version with the existing source is quiet difficult. The risk of Data migration and compatibility are matter in this level. Example; 'Koha' improved new versions are being released frequently and it is difficult to replace with the existing version provided librarian is proficient in it.

3.5 Installation and Customization: Library professionals may not have IT skills sufficient for installation and customization of softwares which makes implementation more a complex process. The basic knowledge of IT may not help in customizing open source software and it requires programming and IT expert involvement in the process.

3.6 Support: Another major risk in open source software environment is, support from the developers or vendors for solving problems at installation level, implementation level and thereafter. Some of the commercial developers and vendor are there to support but the charges are too high. For instance commercial vendors the Nucsoft OSS labs, Bangalore, Informatics India Pvt. Ltd., Bangalore and DELNET, New Delhi, are providing support service across India for KOHA. For installation of KOHA and basic customization including hosting on cloud by Informatics India Pvt. Ltd. Company charges rupees fifty thousand per year as a service charge. The cost for customization of software will differ based on the client requirements.

3.7 Sustainability: Prediction of future development in open source softer is not simple or easy. Sustainability of OSS and its future is not guaranteed, any time anything may happen, like software may crash, errors may occur and software bugs may affect the program. Sustained support from the IT experts is the major risk.

4. Security Measures

OSS implementation and adoption in libraries is a major project and risky too. Librarians need the awareness about present system and about the desired status and what library system is looking for. Some of the security measures required for OSS implementation are-

4.1 Analyze and evaluate the current status: librarian should take steps to analyze the status of current technology being used. While analyzing, comparisons have to be made with new open source software, along with its advantages and disadvantages in terms of technical background. The evaluation should be made consciously on the new open source software keeping in mind the library standards. Evaluation procedures could be-

1. Continuous review of developer’s website.
2. Constant touch with other libraries who have implemented OSS
3. Inviting a commercial vendor to provide a demonstration.
4. Reading reviews on the product
5. Practice of trial and error

4.2 Cost involvement: Cost includes the manpower, training and hardware set up. Real cost involvement has to be measured and planned for the smooth process of the project Implementation.

4.3 Compatibility Test: Compatibility test is needed before implementing new software. It is necessary to test the compatibility of the software with the existing one. Compatibility has to be measured carefully and decision should be taken based on the test.

4.4 Network Security: it is important to establish a security control[ix] system ensuring the protection of OSS network operation to prevent the unauthorized access. Special security measures are to be planned for the protection of data integrity and confidentiality of data transfers through public networks well in advance. New versions of firewalls have to be regularly updated to cope up with the threat of network attacks.

4.4.1 List of reputed firewall softwares[x]

a) Avast! Internet Security
b) AVG Internet Security
c) Comodo Firewall
d) Como do Internet Security Pro
e) iBoss Home Parental Control Router/Firewall
f) Kaspersky ONE Universal Security
g) Lookout for Android
h) Norman Security Suite PRO
i) Norton 360 Version
j) Online Armor Premium Firewall
k) Panda Global Protection
l) Secure IT
m) Secure IT Plus
n) Stop Sign Internet Security
o) Zone Alarm Free Firewall

4.5 Back-up procedure: Taking regular backup of database is a best practice. Proper procedures have to be planned for regular data back up to avoid the data crash or loss. Keeping backup data at different locations (external) rather than storing internally (same server) is a best practice.

4.6 User Access Levels: The user access levels are to be defined by the administrator for the security reasons. To execute control over the software, ability of the users to access or modify or operate, has to be identified and the access levels are to be defined accordingly to protect the system. Administrator has to ensure that the specified privileges are given to staff based on the skills and capability for handling the modules of the software.

4.7 Regular training: OSS is continually being improved upon and regular training is required. The latest happenings on open source softwares can be obtained through workshops, seminars, conferences etc.

4.8 Regular monitoring: Administrator has to perform regular log monitoring[xi] to detect malicious activities and has to take informed decision. Log monitors are type of software that monitors log files, Servers, application, network and security devices. Through log monitors errors, problems, and more information is constantly logged and saved for analysis.

5. Conclusion

There are many security issues and risk factors emerge during the installation and implementation stages. But Library professionals can equip themselves to implement the open source software successfully in the libraries such as Dspace and Greenstone for digital library, Drupal and Zoomla for content management, Koha and NewGenLib for Library Management System. OSS initiations are significant contribution and a strong support for libraries in economizing their expenditure, assisting automation of library functions and services keeping library personnel up to date in technology.

References

1. Chopra, Anil (2012). Information Security Nightmares. PC Quest, May 2012, p32-33.
2. Christian Payne (2002). On the security of open source softwares software, Information Systems Journal;12(1), p 61–78.
3. Fagan, Jody Condit; Keach, Jennifer A. (2010). Build, Buy, Open source softwares, or Web 2.0?: Making an Informed Decision for Your Library. Computers in Libraries; 30(6), p9-11.
4. Griggs, Kim. (2009). Library Information Made to Order: An Open source softwares Project Built for and with Librarians. Computers in Libraries; 29(2), p13-14.
5. Joel West, Scott Gallagher (2006). Challenges of open innovation: the paradox of firm investment in open-source software. R&D Management; 36(3) p319–331.
6. Mickey, B. (2001). Open source softwares and Libraries: An Interview with Dan Chudnov. Weston Then Wilton; 25(PART 1),p23-29
7. Piva, Evila; Rentocchini, Francesco; Rossi-Lamastra Cristina (2012). Is **Open source softwares,** Software about innovation? Collaborations with the **Open source softwares** Community and Innovation Performance of Software Entrepreneurial Ventures; Journal of Small Business Management, 50(2), p340-364.
8. Rapp, D. (2011). Open source softwares Reality Check: Believe the hype or not, implementations of open source softwares integrated library systems have been rocky. Library Journal; 136(13), p34.
9. Rochkind, Jonathan (2008). A Primer in **Risk.** Library Journal; 133(19), p22-25.
10. Sarah McNicol (2005). The importance of evaluation and evidence-based skills to improving service delivery. Library & Information Research, 29(93), p26-34.
11. Soi, Dhruv (2012). 10 Ways to Secure Your Website. PC Quest, May 2012,p53-54.
12. University of Kashmir (2011). Department of Library and Information Science to Organize Three Days National Seminar on Open source softwares Software Systems: Challenges and Opportunities. Trends in Information Management; 6(2), p144-144.
13. Bretthauer, D. (2001). Open Source Software: A History. *UConn Librariess Published Works*(7), 1-20.
14. C, J. T. (2005). Digital Technology and Libraries: a copyright law approach. *Annals of Library and Information Studies, 52*(1), 1-7.
15. http://en.wikipedia.org/wiki/Open_source_software_security
16. http://www.sans.org/reading_room/whitepapers/awareness/security-concerns-open-source-software-enterprise-requirements_1305
17. http://www.slideshare.net/stellacomans/open-source-integrated-library-systems
18. http://www.finance.gov.au/sites/default/files/COV_216905_Risk_Management_Fact_Sheet_FA3_23082010.pdf
19. http://opensource.org/osd