Risk assessment of digital library information security: a case study

Zhengbiao Han, Shuiqing Huang and Huan Li
College of Information Science and Technology, Nanjing Agricultural University, Nanjing, China, and
Ni Ren
College of Information Science and Technology, Nanjing Agricultural University, Nanjing, China and Institute of Agricultural Economics and Information, Jiangsu Academy of Agricultural Sciences, Nanjing, China

Received 12 September 2014
Revised 4 January 2015
1 April 2015
5 June 2015
Accepted 21 June 2015

Abstract

Purpose – This paper uses the GB/T20984-2007 multiplicative method to assess the information security risk of a typical digital library in compliance with the principle and thought of ISO 27000. The purpose of this paper is to testify the feasibility of this method and provide suggestions for improving information security of the digital library.

Design/methodology/approach – This paper adopts convenience sampling to select respondents. The assessment of assets is through analyzing digital library-related business and function through a questionnaire which collects data to determine asset types and the importance of asset attributes. The five-point Likert scale questionnaire method is used to identify the threat possibility and its influence on the assets. The 12 respondents include directors and senior network technicians from the editorial department, comic library, children's library, counseling department and the learning promotion centre. Three different Guttman scale questionnaires, tool testing and on-site inspection are combined to identify and assess vulnerabilities. There were different Guttman scale questionnaires for management personnel, technical personnel and general librarian. In all, 15 management librarians, 7 technical librarians and 72 ordinary librarians answered the vulnerability questionnaire. On-site inspection was conducted on the basis of 11 control domains of ISO 27002. Vulnerabilities were scanned using remote security evaluation system NSFOCUS. The scanning covered ten IP sections and a total of 81 hosts.

Findings – Overall, 2,792 risk scores were obtained. Among them, 282 items (accounting for 10.1 per cent of the total) reached the high risk level; 2 (0.1 per cent) reached the very high risk level. High-risk items involved 26 threat types (accounting for 44.1 per cent of all threat types) and 13 vulnerability types (accounting for 22.1 per cent of all vulnerability types). The evaluation revealed that this digital library faces seven major hidden dangers in information security. The assessment results were well accepted by staff members of this digital library, which testified to the applicability of this method to a Chinese digital library.

Research limitations/implications – This paper is only a case study of a typical Chinese digital library using a digital library information security assessment method. More case-based explorations are necessary to prove the feasibility of the assessing strategy proposed in this study.

Originality/value – Based on the findings of recent literature, the authors found that very few researchers have made efforts to develop methods for calculating the indicators for digital library

The authors gratefully acknowledge the financial support for this study by the national social science fund project of China. Project number is 12ATQ001.

The Electronic Library
Vol. 34 No. 3, 2016
pp. 471-487

0264-0473
DOI 10.1108/EL-09-2014-0158

information security risk assessment. On the basis of ISO 27000 and other related information security standards, this case study proposed an operable method of digital library information security risk assessment and used it to assess a the information security of a typical Chinese digital library. This study can offer insights for formulating a digital library information security risk assessment scale.

Keywords Digital library, Risk assessment, Vulnerability, Information security, Threats

Paper type Case study

1. Introduction

Traditional research on library security is mainly concerned with paper-based information resources security (Bello, 1998;Ajegbomogun, 2004;Holt, 2007) and information systems security (Balas, 2005). Now, it has moved beyond a focus on handling security risk technically to a stage where equal importance is attached to technology and management (Ismail and Zainab, 2013). Compared with traditional library, digital library faces greater security risks due to its high dependence on computer technology, network technology, data communication technology and other high-tech technology. Once problems in information security arise, the operation and the service of the whole digital library system are likely to be affected. It is worth noting that digital library is defined in different ways (Anderson, 1997; Lesk, 1997; James and Thong, 2002). In this research, digital library is restricted to the digital parts built on traditional library, and the digital library information security management refers to the management of the digital parts of traditional library. In preliminary investigation of domestic digital library information security, Huang (2011) indicated that all 30 digital libraries had experienced information security incidents. Among these digital libraries, six had experienced one incident, ten had experienced two and the rest had experienced three or more. However, the information security practice on a specific digital library has been rarely studied. As for digital library organization department, how does the digital library organization department identify rapidly and effectively core assets under potential threats? How do they deal with the threats effectively? How can the management formulate internal policies and documents to guarantee information security? These problems need to be addressed from the perspective of digital library information security risk assessment.

2. Literature review

Literature concerning digital library information security risk assessment mainly deals with four issues, namely, traditional library information security, digital library information security, the standards and specifications of digital library information security management and the information security risk assessment method.

Traditional library information security lays foundation for this study because digital library as a new concept develops from it. The following are some important studies on traditional library information security issues. Maidabino and Zainab (2011) based on a review of library security and security parameters developed a comprehensive instrument for library security management and assessment, as well as a five-factor house model. Balas (2005) analyzed the measures taken to guarantee library computer safety.Ismail and Zainab (2013) propose an library information system security evaluation model, which comprises five components: technological security foundation, information security policy, procedures and control, administrative tools, methods and awareness creation. Abioye and Rasaki (2013) investigated security

challenges in university libraries in Southwest Nigeria, which used questionnaires and interviews to collect data. Fox (2006) and Gressel (2014) emphasized the need to protect the information of library system users. Bowers (2006) proposed that both hacker and government agencies are interested in collecting library users' information. These studies are different from each other, but all agree that library information security problems involve technology, management, users and outside stakeholder (e.g. government agencies) and maintained that library information safety management assessment should be holistically analyzed. The traditional library information security provides a theoretical basis for this study; and the factors, methods and approaches concerning traditional library security can be adopted in the study of digital library information security.

But little was known about research devoted to digital library information security, as early research mainly focused on technical issues. Adam *et al.* (2002) proposed a content-based authorization model for digital libraries. Kuzma (2010) analyzed the vulnerability in European library websites and its effects on user data protection. This research showed that librarians in charge of Web systems did not take appropriate measures to protect their online information systems. Following the tendency to attach equal emphasis to technology and management in the information security domain, Anday *et al.* (2012) reviewed the literature over the 2000-2010 period concerning information security issues ranging from infrastructure, digital content, users and standards and legal issues. They believed that both technology and management play a vital role in digital library security.

For the sake of effective guidance in information security management, it is essential that governments or trade association define standards in digital library information security management. The most important information security management standards are derived from a series of ISO/IEC 27000 of British BS7799. ISO 27001 was specially formulated for risk assessment. ISO 27011 and ISO 27799 are proprietary standards for telecommunication and medical industry. ISO 27015 is proprietary standard for financial industry, which is being developed by ISO. The risk assessment definition of ISO 27000 was cited from ISO Guide 73:2002. Risk assessment includes risk analysis and risk evaluation. The former used information systematically to identify risk sources and estimate the risk, and the latter compares identified risks by given risk criteria so as to assess the risk severity level. In recognition of its security efforts, OCLC has met ISO 27001 security standards and has received registrations. OCLC's ISO 27001 information security management system is aligned with ISO 9001:2000 certified quality processes (www.oclc.org/content/dam/oclc/policies/security/oclcinformationsecuritywhitepaper.pdf). In addition, there is a large amount of literature on library information security risk assessments. Lopez (2003) proposes a physical security control planning framework aiming at the safety tasks of Library of Congress.Michalko *et al.* (2010) mainly examined the greatest risks to research libraries and which of these risks is susceptible to mitigation. The results yielded a shared perspective on a landscape of challenges to US research libraries. Myongho (2011) recommended a library safety guideline that ensures the safety of digital library collections, users and physical structures by combining management, technology and physical entities.

The thoughts and principles of ISO 27000 maintain a certain degree of independence from the specific assessments methods, so ISO 27000 series standards do not specify which kind of risk assessment methods should be adopted. Appendix E of ISO 27005

exemplifies three different assessment methods, namely, value matrix method, threat hierarchical method and risk binary method (ISO and IEC, 2011). Formulated in accordance with the thoughts and principles of ISO 27000, GB/T20984-2007 also proposes two risk assessments methods. Therefore, ISO 27000 series standards can provide technical basis and valuable experience for formulating digital library information security management standards.

Based on previous research and complying with ISO 27000 ideas and principles, this current article adopts GB/T20984-2007 multiplicative method as digital library information security risk assessment method and used it to assess a Chinese public digital library. The purpose of this article is to prove the operability of this method and provide guidance for improving information safety of digital library.

3. Methodology

3.1 Risk assessment object

The object of digital library information security risk assessment is a large-scale public library in Guangdong, also known as one of China's excellent libraries. In 2007 and 2008, it, respectively, won the second session ministry innovation prize of People's Republic of China and international innovation prize of American Library Association (www.cpcss.org/_d271541097.htm). The digital library of this public library has already integrated document lending, information consulting, training and academic research functions, which is typical and representative in China. To understand the information security risk status of the digital library, the administration of the library provided some active co-operations during the assessment process. Therefore, the assessment underwent smoothly and offered findings to advice on digital libraries of the same kind.

3.2 Risk assessment method

ISO 27000 is a widely inclusive international standard. To generalize ISO 27000 series standards in China, Chinese National Bureau of Standards released GB/T20984-2007 in compliance with the principle of ISO 27000 and in light of actual situation of China. GB/T20984-2007 can be used to guide information security risk assessment, identify security correctly and solve information security issues in China.

According to the regulation of ISO 27001, risk value is determined by three indicators, which are asset, threat and vulnerability. However, so far, there are no explicit rules in various standards on how to work out risk values on the basis of the three indicators. Appendix E of ISO 27005 exemplifies three different assessment methods, namely, value matrix method, threat hierarchical method and risk binary method (ISO and IEC, 2011). Formulated in accordance with the thoughts and principles of ISO 27000, Appendix A of GB/T20984-2007 also proposes two risk assessment methods, namely, matrix method and multiplicative method. To some degree, it is fair to say that ISO 27005 and GB/T20984-2007 recommend these methods.

In previous research, we analyzed these methods and other risk assessment methods in everyday work and used them to assess information security of several digital libraries. It proves that GB/T20984-2007 multiplicative method is more suitable for digital libraries than others because $\sqrt{A \times T}$ in multiple multiplicative method restrains asset value and threat contribution to risk value, and it also increases vulnerability contribution to risk value. It is in consonance with the information security situation of digital library. In general, digital library assets are stable. Digital library has

weak control ability on external threats. Compared with threats, digital library managers are more capable of handling safety concerns of assets.

Therefore, this paper uses the GB/T20984-2007 multiplicative method as the digital library information security risk assessment method. The method is shown in equation (1), where R represents the risk value, T refers to the threat level of assets and V means the vulnerability level of assets:

$$R = R(A, T, V) = \sqrt{A \times T} \times V \tag{1}$$

ISO 27000 series standards and GB/T20984-2007 make no provision for assessment of assets, threat and vulnerability, but GB/T20984-2007 proposes that assets, threat, vulnerability and risk level can be assigned by five levels in its body text. Based on the definition of assets, threat and vulnerability in GB/T20984-2007 and risk assessment of telecommunication industry information security (Fan, 2009), this case study puts forward equations (2), (3) and (4) to assess assets, threat and vulnerability. These formulas were used in several digital library information security risk assessments, and they have been proven effective.

Assets are defined as resources that are owned or controlled by digital libraries and that bring social and economic benefits to digital library. Assets assessment takes into account three aspects, that is, the integrity (a_i), the confidentiality (a_c) and the availability (a_a), as shown in equation (2):

$$\mathrm{A} = \frac{a_i + a_c + a_a}{3} \tag{2}$$

When vulnerability exists in digital libraries and security measures are absent, threat acts on assets in a certain way, causing damage and posing information security risk. Suppose A_j related threat is represented by $T(A_j)$, the possibility is Tm, the extent to which integrity, confidentiality and availability of assets are affected are, respectively, represented by T_i, T_c and T_a, then the equation for threats calculating could be expressed as follows:

$$T(A_j) = \sqrt{T_m \times \frac{T_i + T_c + T_a}{3}} \tag{3}$$

Vulnerability refers to the weaknesses likely to be taken advantage of by the threat in assets. There is a many-to-many relationship between vulnerability and threat. In other words, vulnerability may be exploited by multiple threats and a threat may also relate to multiple vulnerabilities. Assume that V represents vulnerability, V_i represents the way i to detect vulnerability and n represents the number of ways to detect each type of vulnerability. The equation for vulnerability calculation is shown as equation (4):

$$V = \frac{1}{n}\sum_{i=1}^{n} v_i \tag{4}$$

3.3 Index assignment and collection methods

We start assets recognition with the businesses and functions of digital library. Having analyzed the assets related to those businesses, we classify and enumerate them to make a list of sorted assets. Then, based on data collected through questionnaires, we define the asset types and the importance of asset attributes. See Huang (2011) for detailed description of assets attributing methods and collecting methods. This paper focuses on the attributing methods and collecting methods concerning threats and vulnerability.

3.3.1 Threat index assignment and collection methods. With reference to the threat classification in "Information Security Risk Assessment Standards for Information Security Technology" of GB/T20984-20984, we take into consideration the actuality of the digital library assets and advice from three experts and, finally, select 52 threats. These threats can be classified into four types, namely, system (10 items), environment (8 items), nature (4 items) and personnel (30 items). These experts are curator, department head and technical librarian of public libraries. They have an intimate knowledge with the potential threats to public digital library. Questionnaires are adopted to control threat data in this study. Considering the actual business process of this digital library, we surveyed department directors and senior network technicians of technology in August 2012. Among the respondents, five are from the network department; the others work in the editorial department, the comic library, the children's library, the department of counseling and the learning promotion center. The threat occurrence possibilities and the assignment method concerning the threat impact on assets are shown in Table I.

3.3.2 Vulnerability index assignment and collection methods. To ensure the accuracy of the investigation, three different methods are used in identification and assessment of vulnerability, namely, questionnaire investigation, on-site inspection and tool test. Responses to the questionnaire can reflect librarians' opinion of this digital library vulnerability status. On-site inspection is conducted by our research team members. The data collected by this method reflects the evaluators' opinion of this digital library vulnerability status. Tool test uses mature software which could determine the digital library real technical vulnerability status.

Questionnaires use Guttman scale form and cover two major types of vulnerability (i.e. technology vulnerability and management vulnerability), as well as some sub-types, as shown in Table II.

Vulnerability questionnaire design is mainly based on vulnerability identification table of GB/T20984-2007 and the business of digital library, which could ensure the validity of the questionnaire. The vulnerability identification table of GB/T20984-2007 covers technical vulnerability and management vulnerability. In pilot investigation, we found that the respondents are only familiar with the duties and businesses of their own department. Especially, management librarians and ordinary librarians have difficulties in understanding the questions of technical vulnerability. Due to the knowledge structure differences among the library staff, we designed three different questionnaires for management librarians, the technical librarians and the ordinary librarians separately. Management librarians include library leaders and department heads, who participated in the investigation about security policies, the responsibilities of the position, safety management, education and training and so on. Technical librarians include technical department members and librarian of other departments in charge of technical work. The investigation of technical librarians involves information

Level	Assignment	Index meaning	Index assignment method
Very high	5	Threats occurrence possibility	High frequency (1 or more times per week); almost inevitable in most cases
		Confidentiality loss rate	Once occurring, it may bring irreparable damage to asset confidentiality and business
		Integrity loss rate	Once occurring, it may bring irreparable damage to asset integrity and business
		Availability loss rate	Once occurring, it may cause very serious damage to asset availability or cause long-lasting intervals
High	4	Threats occurrence possibility	High frequency (1 or more times per month); and it is likely to happen in most case
		Confidentiality loss rate	Once occurring, it may cause serious damage to asset confidentiality and lead to partial function of the asset rights protection system
		Integrity loss rate	Once occurring, it may cause serious and irreparable damage to asset integrity and business
		Availability loss rate	Once occurring, it may cause serious damage to asset availability or long intervals
Medium	3	Threats occurrence possibility	Medium frequency (1 or more times per half year); and it may occur in some cases
		Confidentiality loss rate	Once occurring, it may cause some damage to asset confidentiality and affect the rights protection system
		Integrity loss rate	Once occurring, it may cause some damage to the asset integrity and have effects on the business, but the damage can be fixed
		Availability loss rate	Once occurring, it may bring some damage to the asset availability or cause short intervals
Low	2	Threats occurrence possibility	Low frequency; and unlikely to occur in most case
		Confidentiality loss rate	Once occurring, it may cause minor damage to asset confidentiality and slightly affect the rights protection system
		Integrity loss rate	Once occurring, it may cause minor but tolerable damage to the assets and businesses, but the damage is reparable
		Availability loss rate	Once occurring, it may cause minor damage to asset availability or intervals, which can be repaired right away
Very low	1	Threats occurrence possibility	Threats hardly occur expect in some very rare cases
		Confidentiality loss rate	Once occurring, it may cause negligible damage to asset confidentiality
		Integrity loss rate	Once occurring, it does not affect the asset integrity, and its effect on business can be ignored
		Availability loss rate	Once occurring, it does not affect the asset availability and will not cause intervals

Table I.
Attributing method of threat occurrence possibility and its impact on asset

Table II.
Vulnerability index structure and implementation levels

Vulnerability categories	Vulnerability sub-items	Implementation level
Technical vulnerability		
Physical environments	Fireproofing, power supply and distribution, anti-static precautions, grounding and lighting protection measures of the room	1–Hardly implemented 2 – Having relevant regulations and only some have been implemented 3 – Implemented but not checked 4–Implemented and checked to some extent 5 – Fully implemented good enough to be set as a model for other digital libraries to follow
Network structure	Network structure design, border protection, external and internal access control policy	
System software	Patch installation, physical protection, user accounts, passwords, access control, etc.	
Database software	Patch installation, identification mechanism, password mechanism, access control, backup recovery mechanism, etc.	
Application middleware	Protocol security, transaction integrity, data integrity	
Application system	Audit mechanism, auditing, storage, access control policy, data integrity, password protection	
Management vulnerability		
Technical management	Physical and environmental security, communications and operations management, system development maintenance, access control	
Organizational management	Security policy, organization capability to solve security, asset classification and control, personnel security, compliance with organization	

security management, information security operation maintenance and so on. The ordinary librarians include formal staff of this library who are investigated about responsibilities of the position and operations manual and so on. Altogether 15 management librarians, 7 technical librarians and 72 ordinary librarians were surveyed.

On-site inspection is conducted on the basis of problems concerning the 11 control domain of ISO27002. To check the information security implementation of the digital library in the case study and identify its vulnerability, we visited relevant departments with specific problems in mind. We carried out the inspection in the form of observation, examinations, testing and inquiries. We are mainly concerned with the environments, the implementation, the data documents and the operation habits.

The "remote security evaluation system" of NSFOCUS is used in the vulnerability scanning, which covers IP servers and desktops (www.nsfocus.com.cn/index.html). Relying on professional NSFOCUS security team, this system uses NSFOCUS Intelligent Profile, simulate penetration and other advanced technology comprehensively to find security vulnerabilities of network assets. It is one of the international leading vulnerability management products, which can find these vulnerabilities automatically, efficiently, accurately and timely. Its detection objects include a variety of mainstream operating systems (Windows, Unix, Linux, etc.), application services (FTP, WWW, Telnet, Smtp, etc.) and network equipments.In all, ten IP sections and a total of 81 hosts (servers, storage and network equipment, etc.) are involved in the scanning.

3.3.3 Risk value calculation method. Asset value, threat level and vulnerability are all measured by a five-scale scoring system (1 = very low; 2 = low; 3 = medium; 4 = high; 5 = very high).Here are the specific conversion standards: when $4.2 < \times < = 5$, it is expressed as Level 5.When $3.4 < \times < = 4.2$, it is Level 4. When $2.6 < \times < = 3.4$, it is Level 3.When $1.8 < \times < = 2.6$, it is Level 2, and when $1 < \times < = 1.8$, it is Level 1.The result of value calculation are obtained using multiplicative method of GB/T20984-2007 and range between 1 and 25. Risk is classified into five groups according to its score range and frequency. If the score is located between 1 and 3, then the risk level is 1, which implies that the risk is very low and the business is hardly affected. If the score is located between 4 and 6, then the risk level is 2, which means that the risk is low and acceptable, and the business is a slightly affected. If the score is located between 7 and 9, then the risk level is 3, denoting that the risk is medium, and the business is affected to some extent, but there is no need to take measures. If the score is located between 10 and 14, then the risk level is 4, which means that the risk is high, and the business is affected seriously and measures need to be taken to reduce risk. If the score is located between 15 and 25, then the risk level is 5, which implies that the risk is very high, and the business is affected very seriously and some measures must be taken immediately to reduce risk.

4. Findings

4.1 Threat assessment results

Based on the asset item list and threat sources acquired in the surveys, we propose an assets threats comparison table and, finally, obtained the threat assessment results of the digital library. Partial results are shown in Table III.

Table III shows that the electronic resources of this digital library include purchased resources, self-built resource and Dongguan learning center resources, and they are subject communications failure, storage medium fault, computer equipment failure and

Table III.
Partial results of the threat assessment

Assets categories	Resources	Threats	Occurrence possibility	Security properties loss rate Confidentiality	integrity	Availability	Threats score	Conversion grade
Electronic resources	Purchased resources (e-book, e-journal, dissertation, etc.); Self-built resources (Glorious Image Gallery of Dongguan; Enterprises Database of Dongguan); Other resources(Dongguan learning center, etc.)	Communications failure	3	2	2	3	2.6	2
		Storage medium fault	3	3	4	4	3.3	3
		Computer equipment failure	3	3	3	4	3.2	3
		System software failure	3	3	3	4	3.2	3
		Application software failure	3	3	3	3	3.0	3
		Database failure	3	4	4	4	3.5	4
		Denial of service attacks	3	2	3	3	2.8	3
		Destructive attacks	2	4	4	4	2.8	3
		Unauthorized access	3	4	3	3	3.2	3
		Malicious code	3	4	4	4	3.5	4
		Misuse resource	2	3	3	3	2.4	2
		Internal staff sabotage	2	4	4	4	2.8	3
		Unauthorized data citation or leak	2	4	3	3	2.6	2
		Unauthorized granting of network or device access	2	4	3	2	2.4	2
		Inappropriate configuration and operation	2	2	3	4	2.4	2
		Internal staff personal information loss	2	4	3	3	2.6	2
		Improper hardware maintenance	2	3	4	4	2.7	3
		Improper software maintenance	3	2	3	4	3.0	3
		No or wrong response and recovery	2	2	3	3	2.3	2
		Traffic overload	3	2	2	3	2.6	2
		Supply failure	2	2	2	3	2.2	2
		Inappropriate management and operation	2	3	3	4	2.6	2

other 22 threats. Among these threats, the conversion grade of database failure and malicious code level is 4, which indicates these two digital library threats reach high level. Furthermore, these two threats possibility reaches Level 3, which indicates these two digital library threats has medium frequency(1 or more times per half year), and it may occur in some cases. If these threats occur, then they will exert high-level influence on confidentiality, the integrity and availability of assets. Eventually, according to equation (3), these two threats score is 3.5.

4.2 Vulnerability assessment results

Based on the research of digital library threat list, we propose a threat-vulnerability comparison table and, finally, obtained the assessment results of this digital library vulnerability. Partial results are shown in Table IV.

As shown in Table IV, technical vulnerability of system software includes 11 sub-items such as package installation, physical protection. We obtained the vulnerability assessment of the package installation via three different methods, (i.e. on-site inspection, questionnaire and tool scanning). Using vulnerability assessment method, we get the conversed vulnerability and grade it as Level 3. Risk value distribution is shown in Figure 1.

4.3 Risk scores

Threats are already related with both assets and vulnerability. On this basis, assets, threat and vulnerability are further correlated. Finally, 2,792 risk scores are obtained using the calculation method of risk assessment model. The vast majority of risks are distributed at the very low level (10.53 per cent), the low level (47.67 per cent) or the medium level (31.63 per cent).The results indicate that the information security of this digital library is relatively protected. But there still exist some hidden information security danger. In all, 10.10 per cent of risks reach the high risk level, and measures are needed to reduce the risk. In all, 0.07 per cent of risks attains to the very high level and need to be dealt with in time.

5. Discussion and conclusion

5.1 High risk threat and vulnerability distribution

Two very high-level risk items exist in this digital library and are particularly reflected in physical assets(computer-server, security device-fireproof wall hardware), password attacking threat and software password protecting vulnerability. In addition, some high risks assets include software assets (44.68 per cent), physical assets (31.56 per cent) and electronic resources (23.76 per cent) as major type. The high risk items involve 26 types of threats, accounting for 44.07 per cent of the total. Among them, more than 10 high risk level items correspond to the 12 threat items (including improper hardware maintenance, internal staff sabotage, password attacking, improper software maintenance, malicious infiltrating, invasion and tampering, unauthorized access) individually. The distribution of these threats is shown in Figure 2.

The high risk items fall into 13 vulnerability types, accounting for 22.8 per cent. Among them, more than ten high risk level items correspond to eight threat items (i.e. asset sorting and controlling, security strategies, visit control, back-up and recovery mechanism, system patch installation, software password protection, business continuity and system password strategies) individually. Their distribution is shown in Figure 3.

Table IV.
Partial results of the vulnerability assessment

Vulnerability categories	Vulnerability sub-items	On-site inspection	Questionnaire	Tool scanning	Vulnerability calculation value	Conversed vulnerability grade
Technical vulnerability of system software	Package installation	3	3	2	2.7	3
	Physical protection	2	3	2	2.3	2
	User account	2	3	2	2.3	2
	Password policy	4	3	2	3	3
	Resource sharing	3	2	2	2.3	2
	Event audit	3	2	3	2.7	3
	Access control	3	2	2	2.3	2
	New system configuration	2	2	2	2	2
	Registry reinforcing	2	1	2	1.7	1
	Network security	3	2	2	2.3	2
	System management	3	2	2	2.3	2

5.2 The existence of digital library information security risk

Based on the previous data analysis, we found that the digital library risks are manifested mainly in the following aspects:

- Information security management strategies or mechanism are the guidelines and methodology of library information security management. Due to lack of systematic and independent information security management plans, all important assets are likely to face various threats in every operational stage or worsen the vulnerability in assets even further.
- The access strategies of systems, software, network, database and other important assets are flawed or only partially enforced in some cases. Sometimes, the supervision mechanism does not work sufficiently. All these might cause threats (i.e. network security, improper operation, unauthorized access) to software resources, electronic resources, data files and other forms of assets.

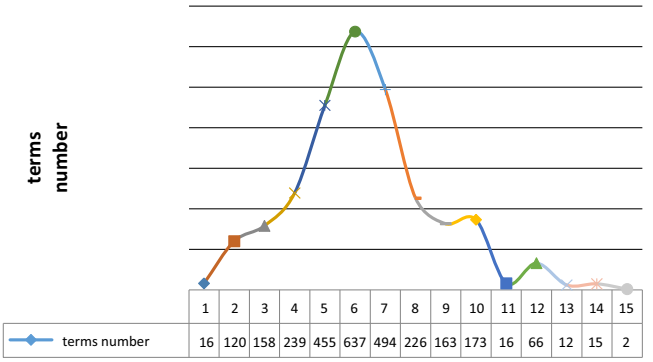

Figure 1.
Digital library information security risk score distribution

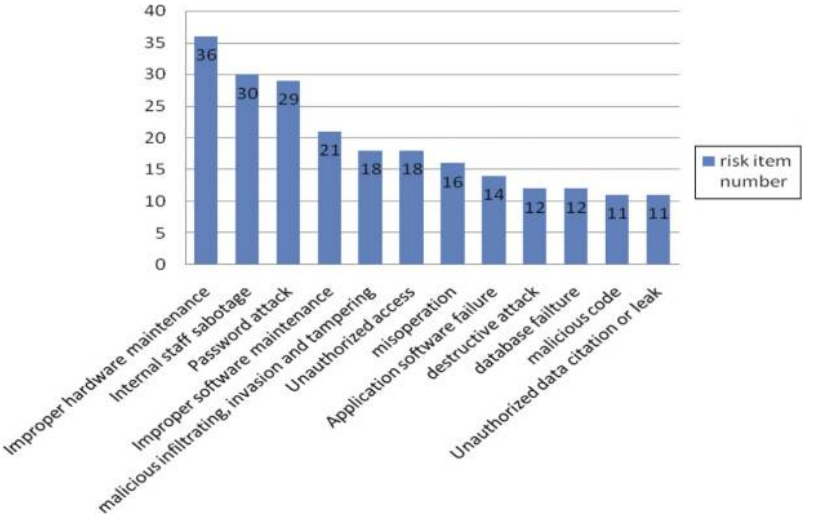

Figure 2.
Threat distributions of high risk items

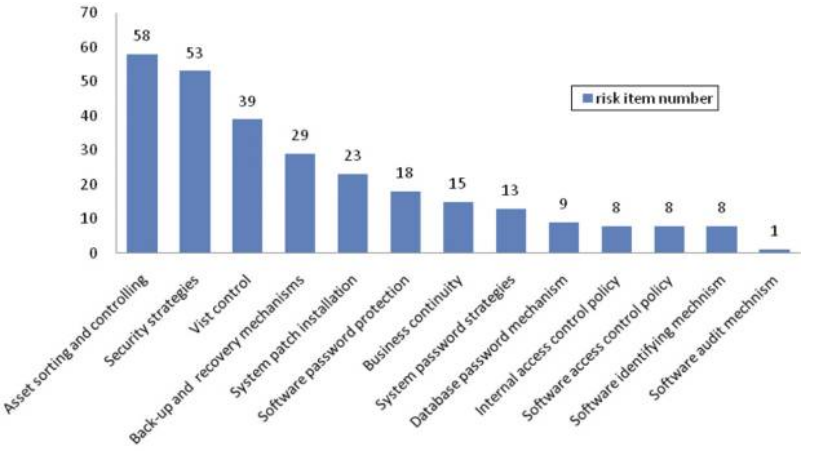

Figure 3.
Vulnerability distributions of high risk items

- Detailed asset sorting and controlling plans, asset management and ownership rights rules are lacking in this digital library; besides, the management is rather inefficient. That would result in threats like poor maintenance and poor management of important hardware assets.
- Backup mechanism is flawed. All the systems and data are backed up locally and are stored in the same computer room. Once a fire, a communication failure or other threats occur, all kinds of facilities, especially the electronic resources and data document assets will be put at serious risk.
- Both servers and personal computers are vulnerable due to delayed updates of systems. Moreover, no strict access control policy is established when systems fail to upgrade in time for certain reasons. Once exploited by hackers, these problems would cause such threats as malicious infiltration, invasion, tampering, malicious code, destructive attack and vulnerability detection to electronic resources, data files and software or hardware.
- As for the servers and the personal servers of this library, there exist vulnerabilities like poor password management, poor identity authentication, unchanged passwords and shared accounts and passwords. All would cause threats like malicious damage, improper operation and misoperation and place electronic resources and data files at risk.
- There is no such measure as business continuity management plans in this library; thus, it is hard to respond quickly and appropriately to the risks once severe information security issues occur.

6. Implication and suggestion

6.1 Practical implication

Based on the risk assessment results and analysis, and considering the current asset operation of this digital library and the safety requirements, we are certain that this digital library should focus on the following risk-control aims:

- Guarantee the physical security of this digital library, that is, the security of various electronic resources, data files, servers, network equipment, office equipment and infrastructure. Protect the library objects from threats of fire, vandalism and mal-operation so as to ensure the normal operation of the digital library.
- Guarantee the system software security of the digital library, that is, the security of portal, service platform, operational system, access control system and business management system and so on. For this purpose, it is necessary to enhance the management in passwords, mails, downloading, software installing of various systems, the management of removable storage media. It is also importance to improve the anti-virus and the anti-attack ability of all systems and increase staff members' safety awareness and operation proficiency.
- Guarantee the safety of the library data, that is, the information safety of all users, staff members and relevant data. To achieve the above aim, it is necessary to enhance password management and train staff intensely in security awareness, operation skills and maintenance knowledge. It is also important to train users more in using and accessing systems.

6.2 Theoretical enlightenment

The fact that the assessment went on well and that, as indicated by our interview, the results are well accepted by both management and technicians verifies the feasibility of the digital library information security risk assessment method adopted in this paper. First, conforming with ISO 27000 series standards, this paper follows the standard principle of risk assessment in terms of methods and process. Second, covering all the digital library assets and the threats and the vulnerabilities they face, this assessment sticks to the holistic principle of risk assessment. Third, high operability of the assessment method and process ensures the completion of the job and also invokes the controllability principle of risk assessment. Fourth, the assessment process meets the principle of minimal influence. Nevertheless, it is important to note that risks control is needed after the completion of assessment, and then, another round of assessing begins. Only different rounds of assessment are carried out, can a high information security level of digital library be maintained. In other words, it is essential to adopt a PDCA cycle mode in managing digital library information security.

Although this research is a case study on a typical domestic digital library information security risk assessment using the multiplication of GB/T20984-2007, the conclusion cannot be extended to other digital library information security risk management. This research finds that assessment of digital library information security involves many types of assets, threat and vulnerability .When correlated with each other, they give rise to 2,792 risks. If such assessment is conducted in all libraries, then it would be very time-consuming considering that respondents have to answer a large number of questions. By conducting more interviews and sending out more questionnaires, we will look further into assets types, assets significance, threat types, threat influence and establish an assessment scale suitable to all libraries, hence increasing the operability and convenience of the digital library assessment mode.

References

Abioye, A.A. and Rasaki, O.E. (2013), "Survey of security challenges in university libraries in southwest Nigeria", *Library & Archival Security*, Vol. 26 Nos 1/2, pp. 1-13.

Adam, N., Atluri, V. and Bertino, E. and Ferrari, E. (2002), "A content-based authorization model for digital libraries". *IEEE Transactions on Knowledge and Data Engineering*, Vol. 4 No. 2, pp. 296-315.

Ajegbomogun, F. (2004), "Users' assessment of library security: a Nigerian university case study", *Library Management*, Vol. 25 Nos 8/9, pp. 386-390.

Anday, A., Francese, E., Huurdeman, H., Yilmaz, M. and Zengenene, D. (2012), "Information security issues in a digital library environment: a literature review", *Bilgi Düünyası*, Vol. 13 No. 1, pp. 117-137.

Anderson, L. (1997), "Digital libraries: a brief introduction", *ACM SIGGROUP Bulletin*, Vol. 18 No. 2, pp. 4-5.

Balas, J. (2005), "Close the gates, lock the windows, bolt the doors: securing library computers", *Computers in Libraries*, Vol. 25 No. 3, pp. 28-30.

Bello, M. (1998), "Library security, material theft and mutilation in technological university libraries in Nigeria", *Library Management*, Vol. 19 No. 6, pp. 379-383.

Bowers, S. (2006), "Privacy and library records", *The Journal of Academic Librarianship*, Vol. 32 No. 4, pp. 377-383.

Fan, Q. (2009), "A research in risk assessment of telecommunication industry information security", *Master Dissertation*, Tianjin University, Tianjin.

Fox, R. (2006), "Vandals at the gates", *OCLC Systems & Services*, Vol. 22 No. 4, pp. 249-255.

Gressel, M. (2014), "Are libraries doing enough to safeguard their patrons' digital privacy", *The Serials Librarian*, Vol. 67 No. 2, pp. 137-142.

Holt, E. (2007), "Theft by library staff", *Bottom Line: Managing Library Finances*, Vol. 20 No. 2, pp. 85-92.

Huang, S. (2011), *Information Security Management of Digital Library*, Nanjing University Press, Nanjing.

Ismail, R. and Zainab, A. (2013), "Assessing the status of library information systems security", *Journal of Librarianship and Information Science*, Vol. 45 No. 3, pp. 232-247.

James, Y. and Thong, H. (2002), "Understanding user acceptance of digital libraries: what are the roles of interface characteristics, organizational context, and individual differences", *International Journal of Human-Computer Studies*, Vol. 57 No. 3, pp. 215-242.

Kuzma, J. (2010), "European digital libraries: web security vulnerabilities", *Library Hi Tech*, Vol. 28 No. 3, pp. 402-413.

Lesk, M. (1997), *Practical Digital Libraries: Books, Bytes, and Bucks*, Morgan Kaufmann Publishers, San Francisco, CA.

Lopez, K. (2003), "Making the library of congress secure: innovation and collaboration", *Journal of Library Administration*, Vol. 38 Nos 3/4, pp. 169-173.

Maidabino, A. and Zainab, A. (2011), "Collection security management at university libraries: assessment of its implementation status", *Malaysian Journal of Library & Information Science*, Vol. 16 No. 1, pp. 15-33.

Michalko, J., Malpas, C. and Arcolio, A. (2010), "Research libraries, risk and systemic change", available at: www.oclc.org/content/dam/research/publications/library/2010/2010-03.pdf?urlm=162937 (accessed 12 May 2015).

Myongho, Y. (2011), "Balanced security controls for 21st century libraries", *Library & Archival Security*, Vol. 24 No. 1, pp. 39-45.

Further reading

General Administration of Quality Supervision (2007), "Inspection and quarantine of the People's Republic of China, standardization administration of the People's Republic of China", GB/T20984-2007 Information security technology-Risk assessment specification for information security, China Standardization Press, Beijing.

Huang, S., Mao, Y. and Xiong, J. (2010), "Assessment of information security risk in digital libraries", *New Technology of Library and Information Service*, Nos 7/8, pp. 33-38.

About the authors

Zhengbiao Han is a Lecturer at the College of Information Science and Technology, Nanjing Agricultural University, Nanjing, China. His current research interests include information security of digital libraries and information user behavior.

Shuiqing Huang is a Professor at the College of Information Science and Technology, Nanjing Agricultural University, Nanjing, China. His current research interests include information security of digital libraries and information retrieval. Shuiqing Huang is the corresponding author and can be contacted at: sqhuang@njau.edu.cn

Huan Li is a Graduate Student at the College of Information Science and Technology, Nanjing Agricultural University, Nanjing, China.

Ni Ren is a Doctoral Student at the College of Information Science and Technology, Nanjing Agricultural University. She is also a Librarian of Institute of Agricultural Economics and Information, Jiangsu Academy of Agricultural Sciences, Nanjing, China.