

Emerald Insight



The Electronic Library

Risk assessment of digital library information security: a case study
Zhengbiao Han Shuiquing Huang Huan Li Ni Ren

Article information:

To cite this document:
Zhengbiao Han Shuiquing Huang Huan Li Ni Ren , (2016),"Risk assessment of digital library information security: a case study", The Electronic Library , Vol. 34 Iss 3 pp. -
Permanent link to this document:
http://dx.doi.org/10.1108/EL-09-2014-0158

Downloaded on: 18 April 2016, At: 23:21 (PT)
References: this document contains references to 0 other documents.
To copy this document: permissions@emeraldinsight.com
The fulltext of this document has been downloaded 21 times since 2016*



Access to this document was granted through an Emerald subscription provided by emerald-srm:512739 []

For Authors

If you would like to write for this, or any other Emerald publication, then please use our Emerald for Authors service information about how to choose which publication to write for and submission guidelines are available for all. Please visit www.emeraldinsight.com/authors for more information.

About Emerald www.emeraldinsight.com

Emerald is a global publisher linking research and practice to the benefit of society. The company manages a portfolio of more than 290 journals and over 2,350 books and book series volumes, as well as providing an extensive range of online products and additional customer resources and services.

Emerald is both COUNTER 4 and TRANSFER compliant. The organization is a partner of the Committee on Publication Ethics (COPE) and also works with Portico and the LOCKSS initiative for digital archive preservation.

*Related content and download information correct at time of download.

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

Risk assessment of digital library information security: a case study

Introduction

Traditional research on library security has been focused primarily on paper-based information resources security (Ajegbomogun, 2004; Bello, 1998; Holt, 2007) and information systems security (Balas, 2005). Recently, researchers have moved beyond a focus on handling security risk in a technical manner to a stage where equal importance is attached to technology and management (Ismail and Zainab, 2013). Compared with a traditional library, a digital library faces greater security risks due to the high dependence on computer technology, network technology, data communication technology, and other high-tech resources. When problems in information security arise, the operation and service of the digital library system are likely to be affected.

It is worth noting that a digital library has several different meanings (Anderson, 1997; James and Thong 2002; Lesk, 1997). In this research, a digital library is restricted to the digital parts built upon a traditional library and digital library information security management refers to the management of the digital parts of a traditional library. In a preliminary investigation of Chinese 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 practices in a specific digital library have rarely been studied. How does the digital library organization department rapidly identify core assets under potential

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

threat? 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.

Literature review

Literature concerning digital library information security risk assessment mainly deals with four issues: traditional library information security, digital library information security, standards and specifications of digital library information security management, and information security risk assessment methods. Traditional library information security lays the foundation for this study since digital library security is developed from previous traditional systems.

Some important studies on traditional library information security issues are presented next. 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) analysed measures taken to guarantee library computer safety. Ismail and Zainab (2013) proposed a library information system security evaluation model which comprised 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 through the use of questionnaires and interviews. Fox (2006) and Gressel (2014) emphasized the need to protect the information of library system users. Bowers (2006) proposed that both hackers and government agencies are interested in collecting library

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

user information. These studies are different from each other, but all agree that library information security problems involve technology, management, users, and outside stakeholders (government agencies, for example), as well as maintained that library information safety management assessment should be holistically analysed. Traditional library information security provides a theoretical basis for this study, as well as the factors, methods, and approaches concerning traditional library security that can be adopted in the study of digital library information security.

Little is known about research devoted to digital library information security since the early research mainly focused on technical issues. Adam *et al.* (2002) proposed a content-based authorization model for digital libraries. Kuzma (2010) analysed vulnerabilities in European library web sites and the effects on user data protection. His 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 associations define standards in digital library information security management. The most important information security management standards are derived from a series of ISO/IEC 27000 standards of the British BS7799. ISO/IEC 27001 was specially

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

formulated for risk assessment. ISO/IEC 27011 and ISO 27799 are proprietary standards for the telecommunication and medical industries. ISO/IEC 27015 is a proprietary standard for the financial industry. The risk assessment definition of ISO/IEC 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 to 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/IEC 27001 security standards and has received registrations. OCLC's ISO/IEC 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) proposed a physical security control planning framework aimed at the safety tasks of Library of Congress. Michalko *et al.* (2010) examined the greatest risks to research libraries and which of these risks was susceptible to mitigation. The results yielded a shared perspective on the landscape of challenges to US research libraries. Myongho (2011) recommended a library safety guideline that helps to ensure the safety of digital library collections, users, and physical structures by combining management, technology, and physical entities.

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

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

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

Based on previous research and complying with ISO/IEC 27000 ideas and principles, this current article adopts the GB/T20984-2007 multiplicative method as a digital library information security risk assessment method and uses 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 the information safety of a digital library.

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

Methodology

Risk assessment object

The object of the digital library information security risk assessment is a large-scale public library in Guangdong, one of China's most excellent libraries. In 2007 and 2008, it won the second session ministry innovation prize of the People's Republic of China and an international innovation prize from the American Library Association (www.cpcss.org/_d271541097.htm). The digital part of this public library has already integrated document lending, information consulting, training, and academic research functions, which is typical for and representative of libraries in China. In order to understand the information security risk status of the digital library, the administration of the library actively cooperated during the assessment process. Therefore,

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

the assessment went smoothly and offered findings which can be used to provide advice to other digital libraries of the same type.

Risk assessment method

ISO/IEC 27000 is a widely inclusive international standard. In order to generalize the ISO 27000 series standards in China, the Chinese National Bureau of Standards released GB/T20984-2007 in compliance with the principle of ISO/IEC 27000 and in light of the 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 ISO/IEC 27001, risk value is determined by three indicators: asset, threat, and vulnerability. However, so far there are no explicit rules in the various standards about how to determine risk values on the basis of the three indicators. As stated previously, Appendix E of ISO/IEC 27005 exemplifies three different assessment methods; namely, the value matrix method, the threat hierarchical method, and the risk binary method. Formulated in accordance with the thoughts and principles of ISO/IEC 27000, Appendix A of GB/T20984-2007 proposes two risk assessment methods; namely, the matrix method and the multiplicative method. To some degree, it is fair to say that ISO/IEC 27005 and GB/T20984-2007 both recommend these methods, respectively.

In previous research, the authors analysed these methods and other risk assessment methods in everyday work, and used them to assess information security of several digital libraries. The previous work showed that the GB/T20984-2007 multiplicative method is more suitable for

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

digital libraries than other methods. This is because $\sqrt{A \times T}$ in the multiple multiplicative method restrains asset value and threat contribution to risk value and increases the vulnerability contribution to risk value. It is in consonance with the information security situation of digital libraries. In general, digital library assets are stable, although they have a weak ability to control external threats. Compared with threats, digital library managers are more capable of handling safety concerns of assets. Therefore, this paper employs the GB/T20984-2007 multiplicative method as the digital library information security risk assessment method. The method is shown in Formula 1, where R represents the risk value, T refers to the threat level of assets (A), and V means the vulnerability level of assets.

$$R = R\left(A,\ T,\ V\right) = \sqrt{A \times T} \times V \qquad \text{(Formula 1)}$$

The ISO/IEC 27000 series standards and GB/T20984-2007 make no provision for the 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 the telecommunication industry information security (Fan, 2009), this case study uses formulas 2, 3, and 4 to assess assets, threat, and vulnerability. These formulas were used in several digital library information security risk assessments and 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 a digital library. Assets assessment takes into account three aspects; that is, integrity (a_i), confidentiality (a_c), and availability (a_a), as shown in Formula 2.

$$\mathrm{A} = \frac{a_{\mathrm{i}} + a_{\mathrm{c}} + a_{\mathrm{a}}}{3} \qquad \text{(Formula 2)}$$

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

When vulnerability exists in digital libraries and security measures are absent, threat acts on assets in a certain way, causing damage and posing an information security risk. Suppose A_j related threat is represented by T (A_j), the possibility is T_m, 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 formula for threats calculation could be expressed as follows:

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

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

$$V = \frac{1}{n}\sum_{i=1}^{n} v_i \quad \text{(Formula 4)}$$

Index assignment and collection methods

The researchers begin asset recognition with the business and functions of the digital library. Having analysed the assets related to those functions, they then classified and enumerated them to make a sorted list of assets. The next step, based on data collected through questionnaires, was to define the asset types and the importance of asset attributes. Huang *et al*. (2010) provided a detailed description of assets attributing methods and collecting methods. This paper focuses on

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

the attributing methods and collecting methods concerning threats and vulnerability.

Threat index assignment and collection methods

With reference to the threat classification in "Information Security Risk Assessment Standards for Information Security Technology" of GB/T20984-2007, the authors considered the actuality of the digital library assets and advice from three experts, and finally selected 52 threats. These threats can be classified into four types: system (ten items), environment (eight items), nature (four items), and personnel (30 items). The experts consisted of a curator, department head, and technical librarian working in a public library. They have an intimate knowledge of the potential threats to public digital libraries. Questionnaires were adopted to control the threat data in this study. Considering the actual business process of this digital library, the researchers surveyed department directors and senior network technicians of technology in August 2012. Among the respondents, five were from the network department and the others worked in the editorial department, the comic library, the children's library, the department of counselling, and the learning promotion centre, respectively. The threat occurrence possibilities and the assignment method concerning the threat impact on assets are shown in Table I.

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

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.

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

		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 cases.
		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 for 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 availability intervals.

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

Low	2	Threats occurrence possibility	Low frequency, and unlikely to occur in most cases.
		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 business, but the damage is reparable.
		Availability loss rate	Once occurring, it may cause minor damage to asset availability for intervals, but can be repaired right away.
Very low	1	Threats occurrence possibility	Threats hardly occur except 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 availability intervals.

Vulnerability index assignment and collection methods

To ensure the accuracy of the investigation, three different methods are used in the identification and assessment of vulnerability: questionnaire investigation, on-site inspection, and tool test. Responses to the questionnaire reflect librarian opinions of the digital library vulnerability status. On-site inspection was conducted by the research team members. The data collected by this

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

method reflects the evaluator opinions of the digital library vulnerability status. Tool test employs mature software, which could determine the real technical vulnerability status of the digital library. The questionnaires used the Guttman scale form and covered two major types of vulnerability (technology vulnerability and management vulnerability), as well as some sub-types, as shown in Table II.

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, and external and internal access control policy.	
	System software	Patch installation, physical protection, user accounts, passwords, access control, and similar.	
	Database software	Patch installation, identification mechanism, password mechanism, access control, and backup recovery mechanism.	
	Application middleware	Protocol security, transaction integrity, and data integrity.	
	Application system	Audit mechanism, auditing, storage, access control policy, data integrity,	

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

		and password protection.	
Management vulnerability	Technical management	Physical and environmental security, communications and operations management, system development maintenance, and access control.	
	Organizational management	Security policy, organizational capability to solve security, asset classification and control, personnel security, and compliance with organization.	

The vulnerability questionnaire design is mainly based on the vulnerability identification table of GB/T20984-2007 and the business of digital libraries, which could ensure the validity of the questionnaire. The vulnerability identification table of GB/T20984-2007 covers technical vulnerability and management vulnerability. In a pilot investigation, the researchers noted that the respondents are only familiar with the duties and operations of his/her own department. For example, administrative librarians and ordinary librarians have difficulties in understanding the questions of technical vulnerability. Due to the knowledge structure differences among the library staff, three different questionnaires were developed to survey administrative librarians, technical librarians, and ordinary librarians, separately. Administrative or management librarians include library leaders and department heads, who participate in the investigation about security policies, responsibilities of the position, safety management, education and training, and so on. Technical librarians include technical department members and librarians in other departments who are in charge of technical work. The investigation of technical librarians involves

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

information security management, information security operation maintenance, and similar. Ordinary librarians include formal staff of the library and are surveyed about the responsibilities of their position, the operations manual, and so forth. Altogether, 15 management librarians, seven technical librarians, and 72 ordinary librarians were surveyed.

On-site inspection was conducted on the basis of problems concerning the 11 control domains of ISO/IEC 27002. In order to check the information security implementation of the digital library in the case study and identify its vulnerability, the researchers visited the relevant departments with specific problems in mind. They carried out the inspection in the form of observation, examinations, testing, and inquiries, mainly concerning the environment, implementation, data documents, and operational habits.

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

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

Risk value calculation method

Asset value, threat level, and vulnerability are all measured by a 5-scale scoring system: (1=very low, 2=low, 3=medium, 4=high, and 5=very high). The specific conversion standards are: when $4.2 < x <= 5$, it is expressed as level 5; when $3.4 < x <= 4.2$, it is 4; when $2.6 < x <= 3.4$, it is level 3; when the value is $1.8 < x <= 2.6$ it is included as level 2; and when it is $1 < x <= 1.8$, it is level 1. The results of the value calculations are obtained using the multiplicative method of GB/T20984-2007 and range between 1 and 25. Risks are classified into five groups according to the score range and frequency. If the score is 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 calculated 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 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 falls between 10 and 14, then the risk level is 4, which means that the risk is high, and the business is seriously affected and measures need to be taken to reduce risk. If the score is between 15 and 25, then the risk level is 5, which implies that the risk is very high, and the business is very seriously affected, and some measures must be taken immediately to reduce risk.

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

Findings

Threat assessment results

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

Table III. Partial results of the threat assessment

Assets categories	**Resources**	**Threats**	**Occurrence possibility**	**Security properties loss rate**			**Threats score**	**Conversion grade**
				Confidentiality	**Integrity**	**Availability**		
Electronic resources	Purchased Resources (e-book, e-journal, dissertation); self-built resources (Glorious Image Gallery of	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

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

	Dongguan; Enterprises Database of Dongguan); other resources (Dongguan Learning Center)	Malicious code	3	4	4	4	3.5	4
		Resource misuse	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

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

Table III shows that the electronic resources of the digital library included purchased resources, self-built resources, and Dongguan Learning Center resources, and that they are subject to communications failure, storage medium faults, computer equipment failure, and 22 other threats. Among these threats, the conversion grade of database failure and malicious code level is 4, which indicates that these two digital library threats reach a high level. Furthermore, these two threats could reach level 3, which indicates that these two digital library threats have medium frequency (1 or more times per half year) and threats may occur in some cases. If the threats occur, they will exert a high-level influence on confidentiality, integrity, and availability of assets. According to Formula 3, the score for the two threats is 3.5.

Vulnerability assessment results

Based on the research of the digital library threat list, the researchers proposed a threat-vulnerability comparison table, and obtained the assessment results of this digital library's vulnerability. Partial results are shown in Table IV.

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	-	2.5	2
	User account	2	3	2	2.3	2

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

	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
	Registry reinforcing	2	1	2	1.7	1
	Network security	3	2	2	2.3	2
	System management	3	2	2	2.3	2

As shown in Table IV, technical vulnerability of system software includes 11 sub-items, such as package installation and physical protection. The researchers obtained the vulnerability assessment of the package installation via three different methods: on-site inspection, questionnaire, and tool scanning. Using vulnerability assessment, they calculated the vulnerability and graded it as level 3. Risk value distribution is shown in Figure 1.

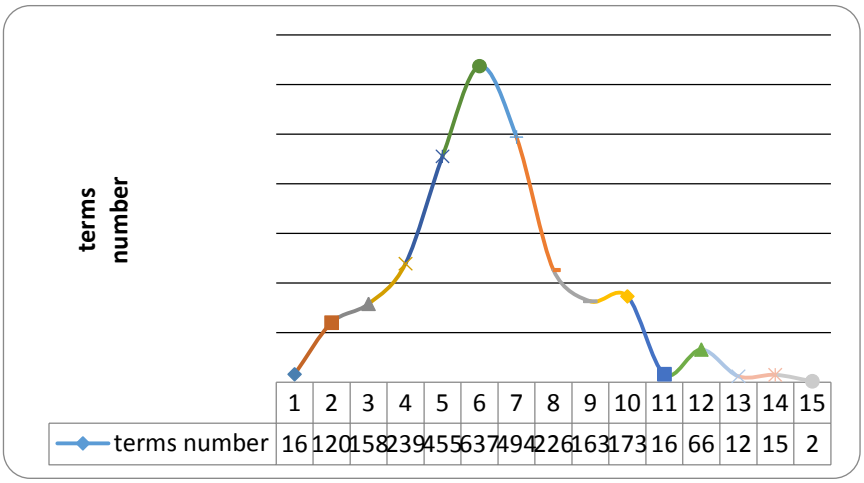


Figure 1. Digital library information security risk score distribution

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

Risk scores

Threats are already related to both assets and vulnerability. On this basis, assets, threat, and vulnerability are further correlated. Using the calculation method of risk assessment model, 2,792 risk scores are obtained. The vast majority of risks are distributed at the very low level (10.5%), the low level (47.7%), or the medium level (31.6%). The results indicate that the information security of this digital library is relatively protected. However, some hidden information security danger exists. High risk level incorporated 10.1 percent of the risks, and measures are needed to reduce the risk. Less than one percent (0.1%) of risks attains the very high level and need to be dealt with in time.

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

Discussion

High risk threat and vulnerability distribution

Two very high level risk items exist in this digital library, and are particularly reflected in physical assets, such as computer-server and security device-fireproof wall hardware, password attacking threat, and software password protecting vulnerability. In addition, some high risk assets include software assets (44.7%), physical assets (31.6%), and electronic resources (23.8%) as major types. The high risk items involve 26 types of threats, accounting for 44.1 percent of the total. Among them, more than ten 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, and unauthorized access)

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

individually. The distribution of these threats is shown in Figure 2.

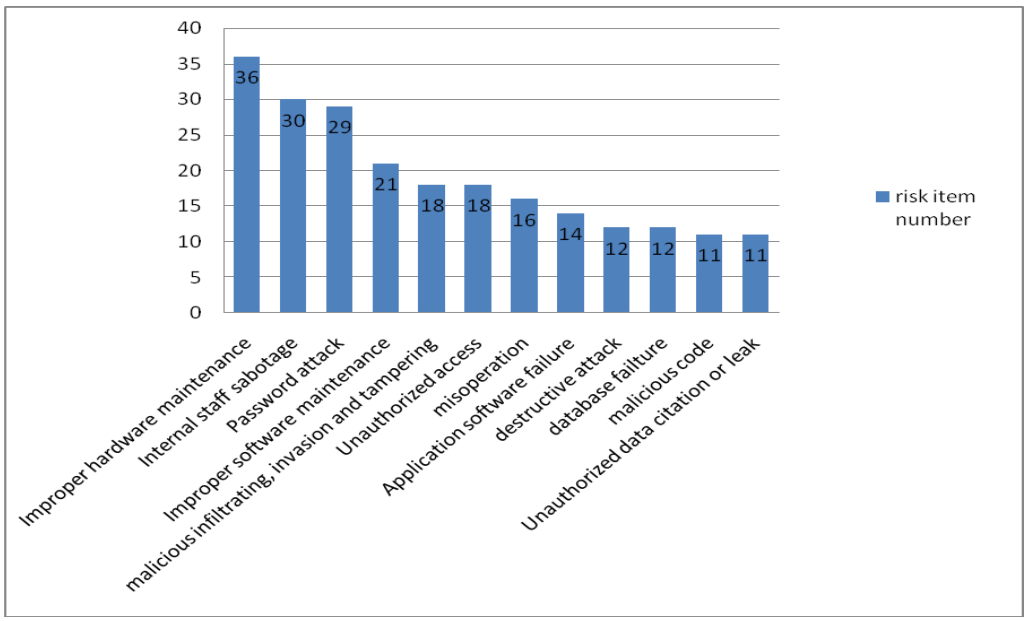


Figure 2. Threat distributions of high risk items

The high risk items fall into 13 vulnerability types, accounting for 22.8 percent. Among them, more than ten high risk level items correspond to eight threat items (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). Their distribution is shown in Figure 3.

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

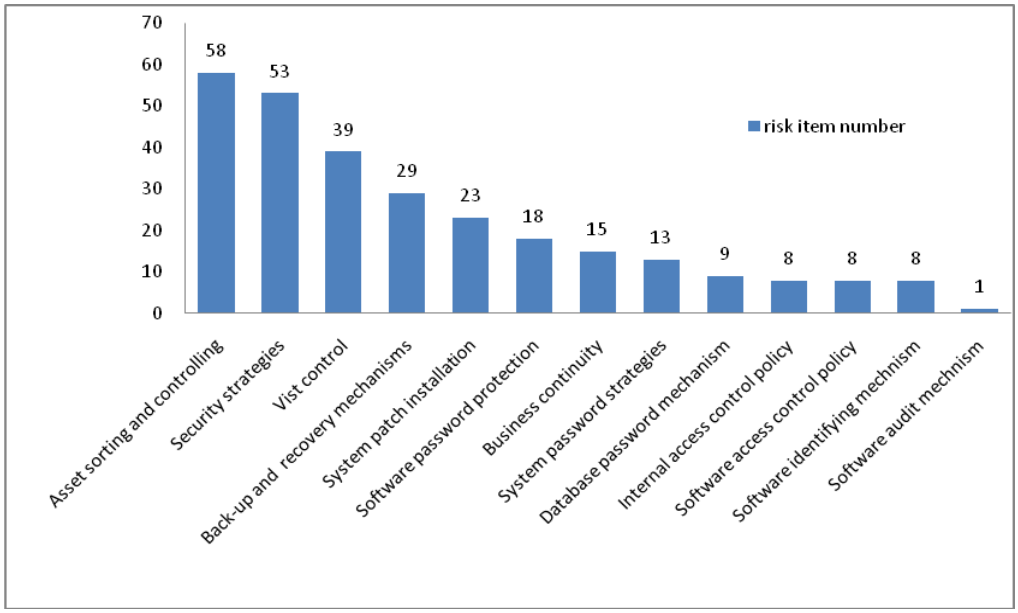


Figure 3. Vulnerability distributions of high risk items

The existence of digital library information security risk

Based on the data analysis, the researchers determined that digital library risks are manifested mainly in the following aspects:

1. Information security management strategies or mechanisms are the guidelines and methodology of library information security management. Due to a 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.
2. 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 of these might cause threats (network security,

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

improper operation, and unauthorized access) to software resources, electronic resources, data files, and other forms of assets.

3. Detailed asset sorting and controlling plans, asset management, and ownership rights rules are lacking in this digital library, and the management is rather inefficient. This results in threats, such as poor maintenance and poor management of important hardware assets.
4. Backup mechanism is flawed. All the systems and data are backed up locally and are stored in the same computer room. Risks, such as a fire, communication failure, or other threats, occur, so all facilities, especially the electronic resources and data document assets, will be put at serious risk.
5. Both servers and personal computers are vulnerable due to delayed updates of the system. Moreover, no strict access control policy has been 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.
6. As for the servers and the personal servers of this library, there exist vulnerabilities, including poor password management, poor identity authentication, unchanged passwords, and shared accounts and passwords. All of these may cause threats, such as malicious damage, improper operation, and misoperation, and place electronic resources and data files at risk.

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

7. There are no 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.

Implications and suggestions

Practical implications

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

1. 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 library objects from threats of fire, vandalism, and mal-operation so as to ensure the normal operation of the digital library.
2. Guarantee the system software security of the digital library; that is, the security of portal, service platform, operational system, access control system, business management systems, and so on. For this purpose, it is necessary to enhance the management of passwords, e-mails, downloading, installation of various systems, and management of removable storage media. It is also important to improve the anti-virus and the anti-attack ability of all systems and to increase staff members' safety awareness and operational proficiency.
3. Guarantee the safety of the library data through protecting the information safety of all

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

users, staff members, and relevant data. To achieve the above aim, it is necessary to enhance password management and train staff in security awareness, operation skills, and maintenance knowledge. It is also important to train users more thoroughly in using and accessing systems.

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

Conclusions and summary

The fact that the assessment went well and that, as indicated by the interview, the results were well accepted by both management and technicians verifies the feasibility of the digital library information security risk assessment method adopted in this paper. Firstly, conforming with the ISO/IEC 27000 series standards, this paper follows the standard principles of risk assessment in terms of method and process. Secondly, by including all digital library assets and the threats and vulnerabilities they face, this assessment sticks to the holistic principle of risk assessment. Thirdly, high operability of the assessment method and process ensures the completion of the job and also invokes the controllability principle of risk assessment. Fourthly, the assessment process meets the principle of minimal influence. Nevertheless, it is important to note that risk control is needed after the completion of an assessment, and then another round of assessing begins. Only when 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 Plan-Do-Study-Act (PDSA) cycle mode when managing digital library information security.

Although this research is a case study of a typical domestic digital library information security risk assessment using the multiplication of GB/T20984-2007, the conclusions may not

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

be extensible to other libraries. However, libraries can learn from the results and look for areas of improvement. 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, 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, the researchers will continue to look further into asset types, asset significance, threat types, and threat influence with the goal to establish an assessment scale suitable to all libraries, hence increasing the operability and convenience of the digital library assessment mode.

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

Acknowledgements

The authors gratefully acknowledge the financial support for this study by the National Social Science Fund Project of China. Project number is 12ATQ001.

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., 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

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

study", *Library Management*, Vol. 25 Nos. 8/9, pp. 386-390.

Anday, A., Francese, E., Huurdeman, H.C., Yilmaz, M. and Zengenene, D. (2012), "Information security issues in a digital library environment: a literature review", *Bilgi Dünyası*, 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.

General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China, Standardization Administration of the People's Republic of China (2007), *GB/T20984. Information Security Technology*. *Risk assessment specification for information security*, China Standardization Press, Beijing.

Fan, Q. (2009), *A Research in Risk Assessment of Telecommunication Industry Information Security*, Master's dissertation, Tianjin University, Tianjin, China.

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

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

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, China.

Huang, S., Mao, Y. and Xiong, J. (2010), "Assessment of information security risk in digital libraries", *New Technology of Library and Information Service*, Vol. 27 Nos. 7/8, pp. 33-38.

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*

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.

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.

Downloaded by The University of British Columbia Library At 23:21 18 April 2016 (PT)

About the authors

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

Shuiqing Huang is a professor at the Information Science and Technology of Nanjing Agricultural University, Nanjing, China. His current research interests include information security of digital libraries and information retrieval.

Huan Li is a graduate student at the Information Science and Technology of Nanjing Agricultural University, Nanjing, China.

Ni Ren is a doctoral student at the Information Science and Technology of Nanjing Agricultural University. She is also a librarian of Institute of Agricultural Economics and Information, Jiangsu Academy of Agricultural Sciences, Nanjing, China.

© Emerald Group Publishing Limited
This is a pre-print of a paper and is subject to change before publication. This pre-print is made available with the understanding that it will not be reproduced or stored in a retrieval system without the permission of Emerald Group Publishing Limited.