Int. J. Pure Appl. Sci. Technol., 29(1) (2015), pp. 1-9

International Journal of Pure and Applied Sciences and Technology

ISSN 2229 - 6107

Available online at **www.ijopaasat.in**

Research Paper

Threat Analysis of Some Information Security Assets in Ibrahim Babangida Library of Modibbo Adama University of Technology, Yola

Daniel Ezra Dzarma[1,*] and Danjuma Jibasen[1]

[1] Department of Statistics and Operations Research, Modibbo Adama University of Technology, Yola, Nigeria

* Corresponding author, e-mail: (dzarma2002@gmail.com)

(Received: 1-10-14; Accepted: 26-6-15)

Abstract: *Ibrahim Babangida Library (IBL), ModibboAdama University of Technology (MAUTECH) Yola faces threats on some Information Security Asset (ISA). Structured questionnaire was administered to library users to obtained data on threats to the IBL. The Annual Loss Expectancy Model (ALEM) was employed. The analysis of the data obtained reveals that the most affected assets in the library of Modibbo Adama University of Technology, Yola are books, which has The Annualized Loss Expectancy (ALE) of N40 000 000, building is second with ALE of N760,323.456 and computer systems is last which have ALE of N80 000. The management were recommended to allocate resources for the threat mitigation in order of ALE priority. The assets with highest ALE should be allocated higher resources.*

Keywords: Annualized Loss Expectancy, Threat Analysis, Information Security assets, Annual Rate of Occurrence.

1.0 Introduction

Libraries, world over are established to meet recreational and educational need of it users. IB library also is not different, the library has collection of materials which meets the recreational needs of its users, enhances research and serve the needs of business men who may require information on trade or commerce to promote their business and to meet the research needs of its users.

However, poor network services has made the library cyber café which supposed to provide relevant information to staff and students' almost redundant, Power fluctuation has led to the underutilization and damages of some information technology equipment as well as losses of some relevant data. The library resource suffers damage due to stealing and mutilation.

Ogbonyomi (2011) states that, the crimes which are committed by some users of the academic libraries, have deprived many others from fully achieving their information needs. Vandalism, mutilation, defacement, theft, arson, etc. are problems regularly encountered by the materials of these libraries. The commodity that libraries promote: books and other information materials are valuable and expensive but are likely targets for criminal activities. The more these materials are safeguarded and secured the more it resembles a library that is traditionally expected to serve its users.

Replacing such materials requires a lot of tax payer money. Measures are usually put in place to checkmate some of the information security breaches by the authority, yet the authority cannot make 100% secure all of the time. Hence, there is a need to evaluate the risk involved.

Insecurity of information is one of the greatest challenges to the information and communication technology (ICT) age. The threat to the security of information do manifest in several ways including:

- The vandalization of communication equipment such as computer system, internet facilities and telephones.
- The loss of some important institutional and personal documents; student’s result, staff bio data and data theft.
- The destruction of some documents and virus infection of some files in a system.
- Disclosure of personal information to unintended persons or group e.g. Health status of an individual, staff payment voucher and pin number.

According to Bogin (2008) even though organizations try to avoid costly information breaches, they cannot make their information 100% secure all of the time. Thus, managing the risk associated with potential information security breaches is an integral part of resource allocation decision associated with information security activities. Of course, to make resource allocation decisions one needs to be clear on what is meant by the term risk.

According to Ajibuwa (2008), information security is the process of protecting data from unauthorized access, use, disclosure, destruction, modification or disruption. The terms information security, computer security and information assurance are frequently used interchangeably. These fields are interrelated and they have common goals of protecting the confidentiality, integrity and availability of information, their differences lie primarily in approach to the subject, the methodologies used and the areas of concentration. Information security is concerned with confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print or other forms.

Threat assessments require a new way of thinking and a new set of skills for criminal justice professionals. These investigations involve analysis of a subject's behaviour and examination of patterns of conduct that may result in an attack on a particular target(s). The level of threat posed by a given subject at a given time becomes a central concern in the investigation and management of the case (Borum *et al*; 1999).

According to Reimer (2010), Implementation of a security program requires an understanding of the nature of information as well as of the systems that require protection and the safeguards suitable to the level and probability of the identified risk.

Information Technology departments are responsible for keeping the security in check, but it is difficult for the organization to get a clear picture of security posture without a formal risk analysis. While IT staff may be competent in implementing security tools, the often lack the expertise in financial modelling and risk analysis. Formal analysis methodology is mature in several fields (finance, engineering, nuclear plant and aviation). However, it is nascent in the information security discipline. Issues with the risk analysis in information security are lack of standardized metrics and processes for evaluation of asset measuring impact of threats and estimating the benefits of controls and acute shortage of data that will enable reasonable statistical analysis to estimate risks. Another problem is the poor quality of data on traits and vulnerabilities that stain from organization fear that revealing security incident will attract other malicious hackers to exploit vulnerabilities and lead to increased frequency of attack.

Just like any other academic library, Ibrahim Babangida Library is faced with the challenges of insecurity of information due to criminal act by users, Anyaobi and Akpoma (2012) asserts that, the abuse of library materials through theft, mutilation and other forms of abuse has posed tremendous challenge to the library profession.

University libraries face a number of security challenges with their collections (both print and non-print). Library collections constitute the bedrock for services provided to the community and serve as important assets to the library. As such, securing and protecting the collections can help libraries provide an effective service in response to the information needs of the university community. Collection security implies the need for libraries to provide, maintain and secure its collection to ensure longetivity, accessibility and effective provision of services to users. To achieve this noble objective however, libraries need an effective strategy to assess the degree of collection security, breaches they are facing and establish an acceptable level of collection security implementation (Maidabinoand Zainab, 2011).

1.1 Operational Definitions

Risk: According to Michaldo *et. al.* (2010), Risk can be defined as the possibility that an event will occur and adversely affect the achievement of the library’s objectives. Security refers to a process designed to protect something or somebody against danger. It is an act of preventing crime, where in the case of library resources; it prevents un-authorized removal or loss of materials, usually as a result of intruders’ or thieves’ interference (Uzuegbuand Okoro, 2012).

Threat: A natural or man-made event that could have some type of negative impact on the organization.

Vulnerability: A flaw, loophole, oversight, or error that can be exploited to violate system security policy.

Technological Hazards: are those hazards resulting from accidents or the failures of systems and structures, such as hazardous materials spills or dam failures.

Human-Hazards: are those hazards resulting from the intentional actions of an adversary, such as a threatened or actual chemical or biological attack or cyber event

ALE is the expected amount to be lost in an organization annually as the result of impact of threat on the asset it is also called loss expectancy.

Asset Value before the Threat (AVB): This refers to the monetary value of the asset before the threat occurs.

Asset Value after the Threat (AVA): This refers to the monetary value of the asset after the threat occurs.

Number of Years Observes (NYO): This refers to the specified periods of time within which the threats are been analysed.

Number of Time (NT) of Occurrence: is the Number of times the threats occur within the number of years observe

2.0 Methodology

Annualized Loss Expectancy (ALE)

Step 1: Single Loss Expectancy (SLE) was computed as the product of Exposure Factor (EF) and the Asset Value Before the threat (AVB). Mathematically

$$SLE = EF \times AVB$$

Step 2: The annualized rate of occurrence estimates how often a threat might be expected to occur, expressed on an annualized basis (for instance threat that is expected to occur once every ten years would have a threat frequency of one tenth or 0.1).

(EF) was computed as the difference between the Asset Value Before threat and Asset Value after the threat divided by the Asset Value Before the threat multiply by 100

$$EF = \frac{AVB - AVA}{AVB} . 100$$

Step 3: Annualized Rate of Occurrence (ARO) was computed as the ratio of Number of the Times (NT) the threat occurs and the Number of Years Observed (NYO).

$$ARO = \frac{NT}{NYO}$$

Step 4: Annualized Loss Expectancy (ALE) was computed as the product of Single Loss Expectancy and Annual Rate of Occurrence:

$$ALE = SLE \times ARO$$

We used ranking scale such as high, medium and low, in the order of their severity such that the assets that has highest ALE was referred to as Asset with Higher risk, the one that was next to it was referred to as medium and the one that had smallest ALE as assets with a lower risk, which is in line with Kindinger and Darby (2000).

3.0 Analysis and Result

Annualized Loss Expectancy of Computer, Books and the Library Building

Table1 gives the summary of ranking ALE of the books, computer resources in Ibrahim Babangida Library and the building structure.

The data in Table 1 were used to compute the ALE of computers which is given in Table 4

Table 1: ALE component of computer systems

Assets	Value
AVB	₦800000
AVA	₦600,000

Depreciation /EF	25%
ARO	4/10

The data in Table 2 were used to compute the ALE of books is given in Table 4

Table 2: ALE component of Books

Assets	Value
AVB	₦500,000,000
AVA	₦50,000,000
Depreciation /EF	10%
ARO	8/10

The data in Table 3 were used to compute the ALE of computers which is given in Table 4

Table 3: ALE component of Building

Assets	Value
AVB	₦76,032,345.60
AVA	₦6,842,911.04
Depreciation /EF	10%
ARO	0.1

The information in the Table 4 shows that building has highest Asset Value Before the threat (₦76,032,345), follow by Books (₦50,000,000) and Computer systems (₦800,000). Computer systems have highest Exposure factor of (25%), books and building have equal Value (10%). Building has the highest Single Loss Expectancy of ₦6,842,911.04 follow by computer systems (₦5,000,000) and computer is last (₦200,000). Books have highest Annual Rate of Occurrence (ARO) of 0.8, followed by Computer (0.4) and building (0.1). Books have highest Annualized Loss Expectancy of ₦40,000,000, Building has moderate ALE of ₦760,323.46 and computer systems have low ALE of₦80,000.

Table 4: The annual Loss Expectancy (ALE) summary for some Library Assets

Asset	AVB	EF	SLE	ARO	ALE
Computer sys	₦800000	25 %	₦2000000	0.4	₦80 000
Books	₦500000000	10 %	₦50000000	0.8	₦40,000,000
Building	₦76,032,345.60	10%	₦6842911.04	0.1	₦684291.104

Discussion

The results show that books have highest risk since it have the highest ALE, this is due to some various crime such as stealing, Mutilation and damages committed by some library users, there are some situation where by some users tear some pages of books, some Reshuffle the books so that other users should not access them and some borrow the books and never return it again. Ogunyade, (2005) states that, theft and mutilation of books are certainly notnew developments of our time. Such acts can be traced as far back as 539BC in Egypt when the Persian conquerors removed rolls of papyri from the library of Ramses II.

The second risky asset is the Library Building; this is because the library building is subject to depreciation and some disasters such as fire outbreak, thunder storm and wind. The management of Ibrahim Babangida library had to reroof the building some years ago because the previous one was linking and causes a lot of havoc.

Even though the computer in Ibrahim Babangida Library are prone to some threats such as Virus infection, hacking and power surge yet it has lowest ALE this is because there are limited number of computer system in the library and they are not fully utilized.

In this research, the data for the analysis were obtained from IB library using Qusestionnaire; the data were analysed using ALE model. The result of the Analysis shows that computer has highest EF of 25%, Books and The Buildings Have equal EF of 10%.

Recommendation

We wish to recommend based on the finding that the management of IBL should;

a. Employ more security personal in the library so as to minimize human threats.
b. Train staff on information security risk management to manage information security risk.
c. Maintain the building and some equipment periodically to forestall further damage
d. Assign securities to each unit in the library.
e. Employ more staff in the library for efficient information management.
f. Re-enforce security measure at the exit to intercept the criminals.
g. Implement disciplinary measure to the defaulters to minimize further breaking of law and order.
h. Ensure constant and steady power supply to the library.

Appendix 1

Information Secrurity Risk Management Analysis: Case Study of Ibrahim Babangida Library of Modibbo Adama University of Technology, Yola

Questionnaire Part 1

1. What is the monetary value of Ibrahim Babangida Library Building?
a. N200 million - N500 million.
b. 100 million - N150 million
c. N600m million - SN900 million.
d. Other please specify…………………………

2. What are the potential threats to Ibrahim Babangida Library Building?
a. Depreciation
b. Fire outbreak
c. Storm
d. All of the above
e. Other Please specify………………………………...

3. With what percentage does the threat has an ability of reducing the value of the library building?

a. 5%
b. 10%
c. 20%
d. 40%
e. Other please specify…………………………

4. How often the Threat likely does occur in 10years?
a. Once
b. Twice
c. Thrice
d. Other specify

Dept.: - - - - - - -
Name: - - - - - -
Post: - - - - - - -
Signature: - - - - - -
Date: - - - - - -

Appendix 2

Part2

1. What is the estimate monetary value of the books in Ibrahim Babangida library?
a. N100,000,000
b. N300,000,000
c. N500,000,000
d. Other please specify ……………………………………………

2. What are the potential threats to the library books?
a. Physical (natural) threat (water, storm, fire outbreak)
b. Cultural (human) events (stealing, mutilation, destruction)
c. Other please specify …………………………………………….

3. The threat or risk has an ability of reducing the values of the books with
a. 10%
b. 20%
c. 30%
d. Other please specify ……………………………………………..

4. How often does the threat occurs in 10years
a. Once
b. Twice
c. Thrice
d. Other specify

Dept.: - - - - - - -
Name: - - - - - -
Post: - - - - - - -
Signature: - - - - - -
Date: - - - - - - -

Appendix 3

Part 3

1. What are the estimates of hardware and software resources in the library?
a. N500,000
b. N1,000,000
c. N10,000,000

2. What are the potential threats to computer facilities in the library?
a. Technological threat (high power voltage virus hacking)
b. Cultural (human) threat (the attitude of students and staff to system)
c. Physical (natural) threat (water linkage storm fire outbreak)
d. All of the above
e. Other specify ……………………………………………………….

3. How often does the threat may likely occur in 10years
a. Once
b. Twice
c. Thrice
d. Other specify

4. With what percentage does the threat may likely reduces the value of computer facilities in the library?
a. 20 – 30%
b. 40 – 50%
c. Other please specify………………………………………………….

Dept.: - - - - - - -
Name: - - - - - -
Post: - - - - - - -
Signature: - - - - - -
Date: - - - - - - -

References

[1] F.O. Ajibuwa, Data and information security in modern day businesses, (Master's Thesis), Atlantic International University, *Abstract International*, 70(2008), 10.

[2] G. Anyaobi and O. Akpoma, Abuse of library materials in academic libraries, *Journal of Research in Education and Society,* 3(2012), 54-58.

[3] R. Borum, R. Fein, B. Vosssekeil and J. Bergvind, Threat assessment, *Behavioral Science and the Law Interscience Journal*, 17(3) (1999), 1-16.

[4] D.L. Bogin, Communication of ACM, University of Meryland, 51(2008).

[5] J.P. Kindinger and J.L. Darby, Risk factor analysis—A new qualitative risk management tool, *Proceedings of the Project Management Institute Annual Seminars & Symposium*, September 7–16 (2000), 959-963.

[6] A.A. Maidabino and A.N. Zainab, Collection security management at university libraries: Assessment of its implementation status, *Malaysian Journal of Library & Information Science*, 16(1) (2011), 1-19.

[7] J. Michaldo, C. Malpas and A. Arcolio, Risk and systemic change, *A publication of Online Computer Library Center (OCLC),* Research Libraries, (2010), 1-20.

[8] T.O. Ogunyade, Theft and mutilation in an academic library: College of medicine, University of Lagos, *Nigerian Quarterly Journals of Hospitals and Medicine*, Medical Library, College of Medicine, University of Lagos, 15(2) (2005), 83-86.

[9] A.L. Ogbonyomi, Security and crime prevention in academic libraries, *Library Philosophy and Practice*, 496(2011), 1-6, http://digitalcommons.unl.edu/libphilprac/496.

[10] R.J. Reimer, Twenty questions directors should ask about information technology security, The CICA's information technology advisory committee, *Library and Archives*, (2010), 1-19.

[11] D. Stonebuner, A. Goguen and A. Faringa, Risk management guide for information, technology system, National Institute of Standard and Technology, (2002), Gaithersburg, http://en.wikipedia.org/wiki/Single.

[12] C.P. Uzuegbu and P.C. Okoro, An x-ray of security practices in Nigerian University libraries, *Greener Journal of Social Sciences*, 2(6) (2012), 197-205.