Security Threats Analysis of Ibrahim Babangida Library, Modibbo Adama University of Technology, Yola

S.S. Abdulkadir and Daniel Ezra Dzarma

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

ABSTRACT: This research work was undertaken to evaluate the problems of Information Security Risk Management of Ibrahim Babangida Library (IBL) of Modibbo Adama University of Technology, Yola. The data for the study were obtained through a structured questionnaire and personal interview from the four Units of the library namely: Readers' unit, serial unit, Reserve Unit and Media Unit. The analysis employed was the Analytic Hierarchy Process (AHP) to prioritized threats in four Units of the library. The analyses of data revealed that: Library Security Threats in IBL are Categorized into three; Technological Threat, Natural Threat and Human Threat. Human Threat is the most severe among the three. Based on this result we gave the Recommendations that management should allocate resources to mitigate information security threat in order of threat preference: Human threat, Technological threat and Natural threats respectively.

KEYWORDS: Data, Analytic Hierarchy Process (AHP), security and threat.

1 INTRODUCTION

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 which include:

The vanderlization 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 systems and disclosure of personal information to unintended persons or group e.g. Health status of an individual, staff payment voucher and pin number.

According to Begin (2008), even though organizations try to avoid costly information breaches, they cannot make their information 100% secure at all times. Thus, managing the risk associated with potential information security breaches is an integral part of resource allocation decision associated with information security activities. 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 data form i.e electronic, print or other forms.

In organization Information Technology (IT) departments are responsible for keeping the security in check, but it is difficult for them to get a clear picture of security posture without a formal risk analysis. While IT staff may be competent in implementing security tools, they often lack the expertise in financial modelling and risk analysis. Similar analysis has been carried out in the area of 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 (Goel, and Chen, 2005).

Academic library in institutions are susceptible to potential criminal problems arising from various forms of undesirable and anti-social activity. This can be well established use of academic libraries by vagrant looking for warm shelter.

Library managers must recognize that wilful criminal damage to buildings and stock is a fact of life and the risk assessment process should take that into account. Criminal damage may happen in variety of forms which range from graffiti, through vandalism, to arson at the extreme end of spectrum. However, library and information managers have also to contend with grey area of damage risk assessment which concerns the very purpose of libraries. Lending materials to users is one of the vital functions of academic library and some of the materials will be costly to replace if damaged either by accident or intent. Library managers must therefore assign priorities in assessing the likely risk of damage occurrence in the process of drawing up the right security strategy for their individual circumstances

Ibrahim Babangida library of Modibbo Adama University of Technology Yola in particular, is facing security challenges just like other libraries, there are some cases whereby students gets into the library and steal some vital materials or documents either in form of a book or paper. There were some situations whereby some students got into the library and tear some pages of books or damage some materials. The study carried out to analyse the risk associated with this kind of problems is known as security risk analysis.

In academic library like Ibrahim Babangida library for instance materials like, books, computers and disks, committee report and recommendations are among several pieces of information that require safety. The question is what can be done to enhance the safety of such important and highly sensitive information? This is indeed within the professional expertise of the Operations Researchers. Incidentally, depth study of every system is one of the best ways to propose a security policy for the system.

An important aspect of information security and risk management is recognizing the value of information and defining appropriate procedures and the protection requirement for the information. Different information requires different degrees of protection. This requires specific information to be assigned specific security classification. The first step in information classification is to identify a member of senior management as the owner of the particular information to be classified. Next, develop a classification policy. The policy should describe the different classification labels, define the criteria for information to be assigned a particular label and list the required security control for each classification. Some factors that influence which classification information should be assigned include how much value that information has to organization, how old the information is and whether or not the information has become obsolete. Laws and other regulatory requirements are also important considerations when classifying information.The collections of libraries are supposed to be made readily accessible to users with the minimum number of rules and regulations. Unfortunately, the popular open door policy to a wide range of readers from different cultures and social backgrounds make libraries vulnerable in the face of increasing anti-social behavior (Quinsee, 1991).

The major objectives of this Research work are: to identify potential information security risk events, prioritise potential risk events and Develop risk management strategies and risk management plan

2 METHODOLOGY

The method used include interview and rating done through Analytical Hierarchical Process AHP to determine the most severe and frequent threat in Ibrahim Babangida Library source of (Technological threat, Natural threat and Human threat) and to prioritize the various threats. Analytic Hierarchy Process is a multiple criteria decision-making tool Saaty (1980). AHP is an Eigen value approach to the pair-wise comparisons. It also provides a methodology to calibrate the numeric scale for the measurement of quantitative as well as qualitative performances. The scale ranges from 1/9 for _least valued than, to 1 for equal, and to 9 for absolutely more important than covering the entire spectrum of the comparison. Some key and basic steps involved in this methodology, are:

1. State the problem.
2. Broaden the objectives of the problem or consider all actors, objectives and its outcome.
3. Identify the criteria that influence the behavior.
4. Structure the problem in a hierarchy of different levels constituting goal, criteria, sub-criteria and alternatives.

5. Compare each element in the corresponding level and calibrate them on the numerical scale. This requires n(n-1)/2 comparisons, where n is the number of elements with the considerations that diagonal elements are equal or 1 and the other elements will simply be the reciprocals of the earlier comparisons.

6. Perform calculations to find the maximum Eigen value, consistency index CI, consistency ratio CR, and normalized values for each criteria/alternative.

7. If the maximum Eigen value, CI, and CR are satisfactory then decision is taken based on the normalized values; else the procedure is repeated till these values lie in a desired range. (Vaidya and Kumar, 2006)

The sample of library staff from readers service unit, serial unit, reserve unit, technical unit, collection development centre, media unit and Physical planning unit of the administrative Block, from Modibbo Adama University of technology were obtained using Stratified sampling procedure. The questionnaires were used to obtain data from the Ibrahim Babangida Library and administrative block of Modibbo Adama University of Technology Yola. It is good to know how the data were analysed or what instruments were used in analysing the data because of the insights its provides into the problem solved or tackled by researchers (Idama 2000). The obtained data were analysed using Analytic Hierarchy Process (AHP) with the aid of Common Gateway (CGI) Software.

This section illustrates how AHP were used to determine weights and prioritize information security threats discovered in Ibrahim Babangida Library of Modibbo Adama University of Technology Yola. The information security threats in Ibrahim Babangida Library were rated using Sa'aty rating scale (1980). Sa'aty's rating scale in Table 1 below was use as a guide to compare the sources of threats.

Table1: Sa'aty;s rating scale

Comparison		Scale
(a)	Equally important	1
(b)	Moderately more important	3
(c)	Essentially more important	5
(d)	Strongly more important	7
(e)	Extremely more important	9
(f)	Intermediate values between two adjacent judgments are	2,4,6,8

Source Saaty 1980

For the purpose of this study, the threats in Ibrahim Babangida Library were categorized into three, namely Human threats (stealing, reshuffles, damage and mutilation), Natural threat (water linkage, thunder and storm) and Technological threat (power surge, virus infection and hacking). Figure 1 illustrates threats functional diagram in IBL
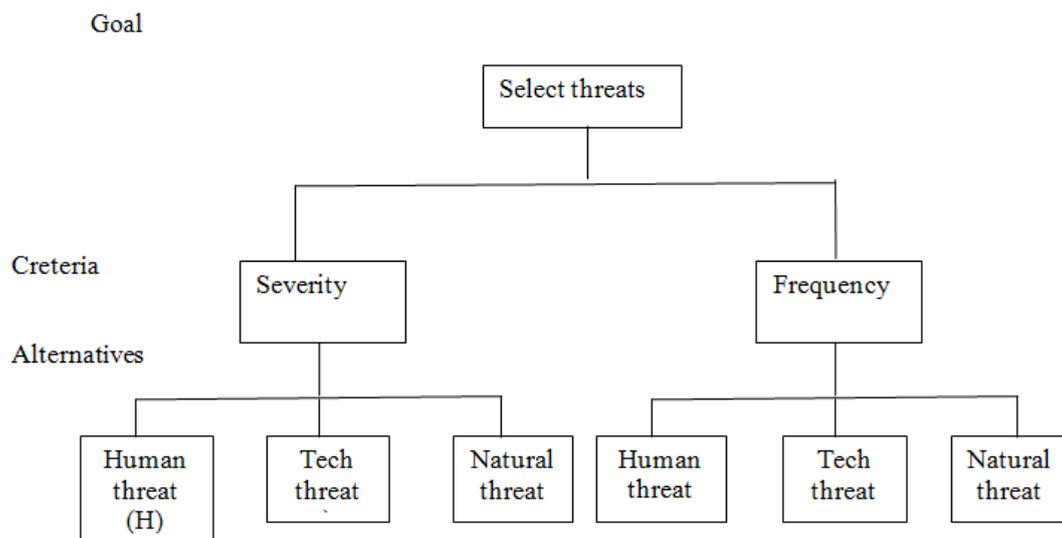
Each of the alternatives were compared from stand point of severity and frequency

Fig 1: Information Security threats functional Diagram of IBL

In order to prioritize the information security threat in Ibrahim Babangida Library the following comparison were made using Sa'aty rating scale as a guide, as illustrated in Table 1

  i.   Severity and frequency
 ii.   Human Threat (T) and Natural Threat (N)
iii.   Human Threat (H) and Technological Threat (T)
 iv.   Technological Threat (T) and Natural Threat (N)

Let A be the threats matrix of Ibrahim Babangida Library.

Hence pair wise comparison matrix of threats in Ibrahim Babangida library

$$
\begin{array}{c}
 \\
H \\
T \\
N
\end{array}
\begin{array}{ccc}
H & T & N \\
\begin{pmatrix}
HH & HT & HN \\
TH & TT & TN \\
NH & NT & NN
\end{pmatrix}
\end{array} \quad \text{Mat. 1}
$$

The weights of Human source of threat (WH), Technological threat (WT) and natural threat (WN) were computed by normalizing and taking the row averages of matrix A.

The consistency Ratio (CR) of Matrix A were computed as follows

$$CR = \frac{\text{Consistency Index (CI)}}{\text{Ratio Index (RI)}}$$

Where

$$CI = \frac{\lambda max - n}{n}$$

$$\lambda max = \sum_{i=1}^{n} AW$$

$$
A = \begin{array}{c}
H \\
T \\
N
\end{array}
\begin{array}{ccc}
H & T & N \\
\begin{bmatrix}
HH & HT & HN \\
TH & TT & TN \\
NH & NT & NN
\end{bmatrix}
\end{array} \quad \text{Mat.2}
$$

$$W = \begin{bmatrix} W_H \\ W_T \\ W_N \end{bmatrix}$$

$$RI = \frac{1.98(n-2))}{n}$$

3   ANALYSIS AND RESULTS

The management of IBL has considered the severity of threats as more critical than frequency of their occurrence. Hence the weight of 0.83 was assigned to severity whereas 0.17 was assigned to frequency of occurrence.

The details of the comparison from the stand point of severity are as shown in Table 2

Table 2: Pairwise Comparison of Three Threats in the library from the standpoint of severity

Pairwise Comparison	More important criterion	How much more important	Numerical Rating
H-T	H	Human threat is equally to moderately more important than technological threat	2
H-N	N	Human threat is moderately more important than natural threat	3
T-N	T	Technological threat is equally moderately important than natural threat	2

Where H= Human Threats, T= Technological Threats, N= natural Threats

The Pairwise Comparison Matrix of Human Threats

$$
\begin{array}{c}
\begin{array}{ccc} H & T & N \end{array} \\
\begin{array}{c} H \\ T \\ N \end{array}
\begin{pmatrix}
1 & 2 & 9 \\
\dfrac{1}{2} & 1 & 2 \\
\dfrac{1}{9} & \dfrac{1}{2} & 1
\end{pmatrix}
\end{array}
\qquad \text{Mat.3}
$$

The CGI software were used to determine the weight associated with H, T and N as shown below

Maximum Eigen Value =3.07351, C.R.= 0.05569, Weights (Eigen Vector)

H= 0.654807, T=0.24856, N= 0.0953377

Among the various threat identified namely; Haman threat, Natural threat and technological threat, the most frequent and severe one is human threat which has the maximum weight 0.654807 followed by the technological threat 0.249856 and finally natural threat which has the weight of 0.0953377. For most covered entities, human threats will be of greatest concern, because human threats have the potential to be triggered or exploited more frequently than natural or environmental threats (*Six Basics of Risk Analysis and Risk Management, 2007*)

 Since the consistency index C.R. = 0.05569 which is less than 0.10 the level of inconsistency is acceptable.

The pairwise comparison between the three threats from standpoints of frequency is as shown in table 3.

Table 3: Pairwise Comparison of Three Threats in the library from standpoints of frequency

Pairwise Comparison	More important criterion	How much more important	Numerical Rating
H-T	H	Human threat is Strongly more important than technological threat	7
H-N	H	Human threat is essentially more important than natural threat	5
T-N	T	Technological threat is equally moderately important than natural threat	3

The Pairwise Comparison Matrix of three Threats from standpoint of frequency

$$
\begin{array}{c}
\begin{array}{ccc} H & T & N \end{array} \\
\begin{array}{c} H \\ T \\ N \end{array}
\begin{pmatrix}
1 & 7 & 5 \\
\dfrac{1}{7} & 1 & 3 \\
\dfrac{1}{5} & \dfrac{1}{3} & 1
\end{pmatrix}
\end{array}
\qquad \text{Mat.3}
$$

The weight associated with H, T and N by normalizing mat.3 and taking the row average.

H = 0.715, T = 0.186 and N = 0.0967

The result shows that human threats has great weight of 0.75, folloowed by Technological threats (0.186) and natural threats is last.

Overall priority of Threats in IBL

Goal

```
                              ┌─────────────────┐
                              │  Select threats │
                              └─────────────────┘
```

Creteria

```
        ┌─────────────┐                      ┌─────────────┐
        │   S=0.83    │                      │   F= 0.17   │
        └─────────────┘                      └─────────────┘
```

Alternatives

```
┌──────────┐ ┌──────────┐ ┌──────────┐ ┌──────────┐ ┌──────────┐ ┌──────────┐
│ H=0.655  │ │ T=0.250  │ │ N=0.715  │ │ H=0.715  │ │ T=0.186  │ │ N=0.0967 │
└──────────┘ └──────────┘ └──────────┘ └──────────┘ └──────────┘ └──────────┘
```

```
┌───────────────────────────┐ ┌──────────────────────────┐ ┌───────────────────────────┐
│ H: 0.83×0.65+0.17×0.715   │ │ T: 0.83×0.250 +0.17×0.186│ │ N: 0.83×0.095+0.17×0.967  │
│ =0.6655                   │ │ =0.24                    │ │ =0.095                    │
└───────────────────────────┘ └──────────────────────────┘ └───────────────────────────┘
```
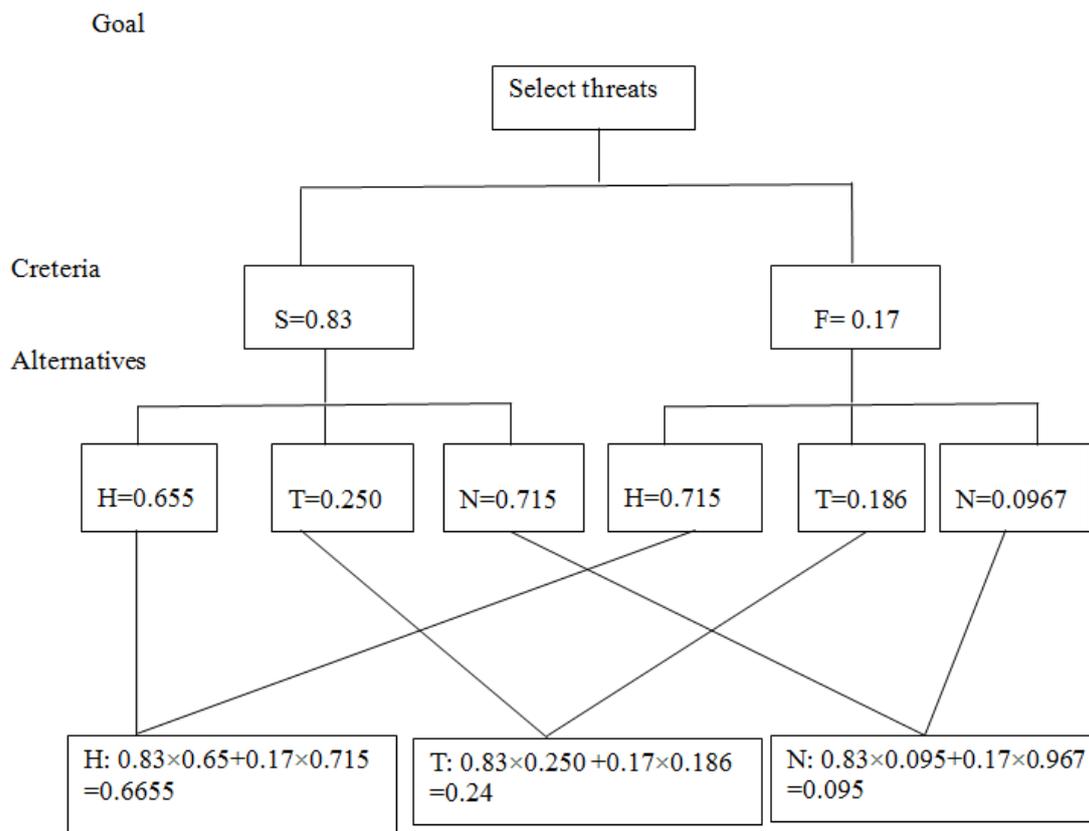
Where S= Severity of threats and F= the Frequency of occurrence of threats

H, T and N are as defined earlier.

The overall priority show that has the highest weight of 0.6655, followed by Technological threat 0.2400 and natural threat 0.095 is last. Human threats in library comprises of stealings, mutilations, vandalisms and so on as.

A number of studies have described how crimes and security breaches incidences can affect the provision of library services to users. Lorenzen (1996) and Holt (2007) identified several such incidents, (i) theft of physical materials; (ii) theft or alteration of data; and (iii) theft of money as major security crime in libraries. Other forms of breaches include non-return of items by borrowers, theft of library equipment, personal theft (from staff and users), verbal and physical abuse against staff and users, and vandalism against library buildings, equipment and stock destruction, all of which can directly or indirectly affects the provision of library services (Ewing 1994). Similarly, Lorenzen (1996) reported how different forms of collection mutilation such as underlining and highlighting text in library books, tearing and or removing pages of books and annotating in books margins can temper with the subject-content of library collection, thereby making it unusable to users. Ajegbomogun (2004) identified the types of security breaches in university libraries, which included theft and book mutilation and reasoned the cause to security lapses, insufficient or limited number of essential materials, and user's financial constraints. Studies conducted by Ajegbomogun (2007), Bello (1998), and Holt (2007) identified rare books, manuscripts and special collections as frequent target of theft and mutilation because of the special demand for in depth studies of such materials. Ewing (1994) identified abuses in UK libraries, which included book and non-book theft, non-return of borrowed items, verbal and physical abuse, and vandalism against library buildings and properties. Abifarin (1997), Allen (1997) and Bello (1998) reported high rate of book theft, mutilation and misplacing of books in Nigerian academic libraries. They suggested measures to reduce the problems, which include tightening security at library entrances and exits, expulsion of students involved in theft and mutilation, provision of multiple copies of heavily used text, reducing the cost of photocopying, and periodic searching of students hostels and staff offices. Atkins and Weible (2003) believe that successful inventorying process helps identify missing items; however it may be dependent on the size of the library's collection (Maidabino and Zainab, 2011)

The aim of this paper was to analyse the information security risk of Ibrahim Babangida Library of Modibbo Adama University of technology, Yola, so as to identify potential information security threat event, prioritise potential threat events, and develop strategy and plans for casting risk management strategies. We identified the information security threat by

using questionnaire to obtain data from the study area. We used AHP to prioritize the threat. That Human threats, Technological threat and Natural Threats.

4 RECOMMENDATION

The following Recommendations have been made based on the findings of this study:

The management of Ibrahim Babangida library 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, to insure implementation of law and order.
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.

REFERENCES

[1] Abifarin, A. (19970). Library stock security: The experience of the University of Agriculture Abeokuta, Nigeria. Library and Archival Security, Vol.14, no.1: 11-19.
[2] Adio, G. and Olasina, G. (2014). Role of library in educational development. Unpublished manuscript.
[3] Ajibuwa F. O. Data and Information Security in Modern Day Businesses. (master's thesis, Atlantic International University, 2008) Abstract international 70, 10.
[4] Ajegbomogun, F.O. (2004). Users' assessment of library security: A Nigerian university case study. Library Management, Vol.25, no.8/9: 386-390.
[5] Al-Habra K. M. A. (2001). Application of the AHP in project management, *International Journal of Project Management* 19. 19-27
[6] Allen, S.M. (1997). Preventing theft in academic libraries and special collections, Library Archives & Security, Vol.14, no.1: 29-43.
[7] .Atkins, S.S. and Weible, C.L.(2003). Needles in a haystack: Using interlibrary loan data to identify materials missing from a library's collection. Library Collections, Acquisitions, & Technical Services, Vol.27: 187-202.
[8] Bello, M.A.(1998). Library security, material theft and mutilation in technological university libraries in Nigeria. Library Management, Vol.19, no.6: 379-383.
[9] Bogin, D.L (2008), Communication of ACM, vol, 51. University of Meryland.
[10] Ewing, D. (1994). Library security in the UK: are our libraries of today used or abused? Library Management, Vol.15, no.2: 18-26.
[11] Holt, G.E. (2007). Theft by library staff. The bottom line: managing library finances, Vol.20, no.2: 85-92.
[12] Goel, S.and Chen, V. (2005),Information Security Risk Analysis- A matrix-based approach, unpublished manuscript
[13] Idama A. (1999), Understanding Operations Research, 1st edition. Paraclete Publishing House Jimeta Yola pg 125.
[14] Lorenzen, M. (1996). Security issues of academic libraries. ERIC Document. No. ED396765.
[15] O'Brien J.A (2004). Management Information System, 6th edition, McGraw-Hill companies, United Stated of America pp G5-9
[16] T.L. Saaty (1980), The Analytic Hierarchy Process, McGraw-Hil companies, United Stated of America.
[17] Saaty T.L. (1980). "The Analytical Hierarchy Process, Planning, priority, resource allocation". RWS Publications, USA
[18] *Six Basics of Risk Analysis and Risk Management 2007*, HIPAA Security Series, U.S.A. Volume 2 , pp 6.
[19] Senyah, Y. and Lamptey B. R. (2014). Personal security and safety in academic libraries: a case study of the Kwame Nkrumah University of science and technology library, Kumasi, Ghana. Unpublished manuscript.
[20] Quinsee, A. G (1991), Introduction, insecurity in academic and research libraries. Manuscript
[21] Vaidya, O. S. and Kumar, S. (2006). Analytic hierarchy process: An overview of applications, European Journal of Operational Research 16 , 1–29.