$$A = \begin{array}{c} \\ p \\ H \\ V \\ N \end{array} \begin{array}{c} \begin{array}{cccc} P & H & V & N \end{array} \\ \begin{bmatrix} PP & PH & PV & PN \\ HP & HH & HV & HN \\ VP & VH & VV & VN \\ NP & NH & NV & NN \end{bmatrix} \end{array}$$

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

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

3. Analysis and Result

In order prioritize the Technological information security threat in Ibrahim Babangida Library the following Pairwise comparison were made between the follow threats: Power surge (P), Hacking (H), Virus (V) and Network failure (N) using Sa'aty rating scale as a guide, as shown in the table 1.The Pairwise comparison matrix between the four Technological threats from standpoint of severity were obtained from table 2.

Pairwise comparison matrix of technological threats from standpoint of severity

$$S = \begin{array}{c} \\ P \\ H \\ V \\ N \end{array} \begin{array}{c} \begin{array}{cccc} P & H & V & N \end{array} \\ \begin{bmatrix} 1 & 7 & 3 & 1/2 \\ 1/7 & 1 & 1/2 & 1/3 \\ 1/3 & 2 & 1 & 1/5 \\ 2 & 3 & 5 & 1 \end{bmatrix} \end{array}$$

The weight for P, H, V and N were obtained by normalizing the threat comparison matrix and taking the average of each row

P= 0.3470, H= 0.0836, V= 0.1134 and N= 0.4560
Consistency Ratio = 0.0992

Since the consistency ratio is less than 0.1 (CR< 0.1) the level of the inconsistency is acceptable.

The result shows that Network failure (0.4560) is the most severe Technological threat followed by Power surge (0.3470), Virus (0.1134) and Hacking (0.0836) is last.

Table 2: The Pairwise comparison of Technological Threats from standpoint of severity

Pairwise Comparison	*More Important Criterion*	*How much more important criterion*	*Numerical Rating*
P-H	P	Strongly More	7
P-V	P	Moderately more important	3
V-H	V	Equally important to moderately more important	2
N-P	N	Equally important to moderately more important s	2
N-H	N	moderately more important	3
N-V	N	Essentially more important	5

The Pairwise comparison matrix between the four Technological threats from standpoint of frequency were obtained from table 3

Pairwise comparison matrix of technological threats from standpoint of frequency

$$F = \begin{array}{c} \\ P \\ H \\ V \\ N \end{array} \begin{array}{c} \begin{array}{cccc} P & H & V & N \end{array} \\ \begin{bmatrix} 1 & 2 & 1/2 & 1/2 \\ 1/2 & 1 & 1/3 & 1/3 \\ 2 & 3 & 1 & 2 \\ 2 & 3 & 1/2 & 1 \end{bmatrix} \end{array}$$

The weight for P, H, V and N were obtained by normalizing the threat comparison matrix from standpoint of frequency and taking the average of each row

P= 0.187, H= 0.108, V= 0.412 and N= 0.293

Consistency Ratio = 0.028

Since the consistency ratio is less than 0.1 (CR< 0.1) the level of the inconsistency is acceptable.

The result shows that virus (0.412) is the most frequent Technological threat followed by network failure (0.293), power surge (0.187) and Hacking (0.108) is last.

Table 3: The Pairwise comparison of Technological Threats from standpoint of frequency

Pairwise Comparison	*More important criterion*	*How much more important criterion*	*Numerical Rating*
P-H	P	Equally to moderately more important	2
P-V	V	Equally to moderately more important	2
H-V	V	moderately more important	3
H-N	N	moderately more important	3
N-P	N	Equally to moderately more important	2
N-V	V	Equally to moderately more important	2

4. Discussion

The result of the analysis from the standpoint of severity indicates that consistency ratio is 0.0992, which indicates that the level of inconsistency in judgement is acceptable. According to Taha 2000, if CR≤ 0.1, the level of the inconsistency is acceptably; otherwise, the inconsistency is high and the decision maker is advised to check the pairwise comparison elements to produce a more consistent matrix. Since CR is 0.0992 the consistency of the judgement is acceptable. The result also reveals that network failure has the highest weight of 0.4560; this could be because the internet service provider does not provide effective internet service or university library

does not have quality facility such as satellite and router to receive the internet service network. Power surge which has weight of 0.3740 is second, this may be because of the power instability from the power provider and lack of facilities such as stabilizer, surge suppressor and transformer to regulate amount of power supply to the library. Kozhiparambil **(**2011), list some possible causes of power surges as follows: Switching of lighting and the starting and stopping of motors, Electrical fault conditions (equipment failure which passes high currents to ground or from phase to phase), Power failure and the subsequent return of power, Lightning strikes that hit the electrical system in nearby geographical area, Lightning strikes that induce transients through radiation of electromagnetic fields (without hitting the electrical system). Peak current for lightning strikes generally range from 2000 to 400,000 amps. The strongest strikes for three phase systems will induce currents of up to 320,000. Computer virus has the third weight of 0.1134; these viruses are contacted from the internet and the use of un scanned devices. Hacking has the least weight of 0.0836; this may be because the library has poor internet services which are not favourable for hackers.

Based on the standpoint of frequency virus (0.412) is the most frequent threat, followed by network failure (0.293), next to it is power surge (0.187) and hacking is last. The level of the inconsistency is also acceptable because CR<0.1.

5. Conclusion

In this paper we identified four major technological threats in Ibrahim Babangida Library of Modibbo Adama University of Technology Yola; power surge, hacking, viruses and network failure through the use of questionnaire and personal interview. The four threats were analysed using Analytical Hierarchical Process (AHP) and the result shows that network failure is the severest, power surge from standpoint of severity while virus is the most frequent threat from standpoint of frequency.

6. Recommendation

The management of Ibrahim Babangida Library is recommended to do the following in order to mitigate the threats:

1) Use stabilizer, power arrestor, power suppressor and assign an electrician to control the power supply
2) Choose a very good Internet Service Provider (ISP) and obtained a better internet gargets.
3) Installed a very effective anti-virus and always scanned any device before using.
4) Screen the users of internet facility

Reference

[1] Ajibuwa, F. O. (2008).Data and Information Security In Modern Day Businesses. Master's Thesis; http //www.AIU.edu.com.

[2] Bonnette C. A. (2003)**.** Assessing Threats to Information Security In Financial Institutions. SANS Institute 2003, GSEC practical assignment. Version 1.4b - Option 1

[3] Bagchi, K., and Udo, G. (2003). "An Analysis of the Growth of Computer and Internet Security Breaches," Communications of the AIS (12), pp. 684-700.

[4] Baskerville, R. (1993). "Information Systems Security Design Methods: Implications for Information Systems Development," ACM COMPUTING SURVEYS (25:4), PP. 375-414.

[5] Computer Economics.(2007). "Annual Worldwide Economic Damages from Malware Exceed $13 Billion," June (http://www.computereconomics.com/article. cfm?id=1225).

[6] Carver, C. S., and White, T. L. (1994). "Behavioral Inhibition, Behavioral Activation, and Affective Responses to Impending Reward and Punishment: The BIS/BAS Scales," Journal ofPersonality and Social Psychology (67), pp. 319-333.

[7] Duggan, D. P. and Michalski, J. M. (2007). Threat Analysis Framework. Sandia Report, Sandia National Laboratories Albuquerque, New Mexico Livermore, California.

[8] Dhillon, G., and Backhouse, J.(2000). "Information System Security Management in the New Millennium," Communications of theACM (43:7), pp. 125-128.

[9] Elliot, A. J. (2006). "The Hierarchical Model of Approach–Avoidance Motivation," Motivation and Emotion (30), pp. 111-116.

[10] Elliot, A. J., and Covington, M. V. (2001). "Approach and Avoidance Motivation," Educational Psychology Review (13:2), pp. 73-92.

[11] Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Richardson, R. (2006)."2006 CSI/FBI Computer Crime and Security Survey," Computer Security Institute (http://i.cmpnet.com/gocsi/db_area/ pdfs/fbi/FBI2006.pdf).

[12] Kozhiparambil K. P (2011), Surge Resistant Uninterruptible Power Supply, The University of Waikato, Waikato.

Loch, K. D., Carr, H. H., and Warkentin, M. E. (1992). "Threats to Information Systems: Today's Reality, Yesterday's Understanding," MIS Quarterly (16:2), pp. 173-186.

[13] Liag, H., and Xue, Y. (2009), Avoidance of Information Technology Threats: A Theoretical Perspective. MIS Quarterly Vol. 33 No. 1/March 2009

[14] Prasad, N.R. (2007). "Threat Model Framework and Methodology for Personal Network", Communication Systems Software and Middleware, COMSWARE 2007.

[15] Stafford, T. F., and Urbaczewski, A. (2004). "Spyware: The Ghost in the Machine," Communications of the AIS (14), pp. 291-306.

[16] Straub, D., and Welke, R. (1998). "Coping with Systems Risk: Security Planning Models for Management Decision Making,"MIS Quarterly (22:4), pp. 441-469.

[17] Taha, H. A. (2000). Operations research an introduction, 6th edition, Fayettevile Prentice-Hall, NewDelhi India, pg 519-526