International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

The Technological Threats of Information Security Analysis in Ibrahim Babangida Library of Modibboadama University of Technology, Yola

Dzarma Daniel Ezra[1], Linus Uwemedimo Udoh[1], N. D. Oye[2]

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

Abstract: ***In this paper the Technological threats of Information Security Analysis in Ibrahim Babangida library of Modibbo Adama University of technology, Yola, the data were obtained using structured questionnaire and personal interview. The threats identified were Power surge, Hacking, Computer Viruses and Poor internet Network services. The data were analysed using Analytic Hierarchy Process (AHP). The result of the analysis from the standpoint of severity revealed that Network failure which has weight of 0.4560 is the severest threat, next to it is Power surge (0.3470), followed by Computer virus (0.113) and hacking (0.0836) is last. The Consistency Ratio (CR) also was computed to be 0.0992 which indicated that the level of the inconsistency of the judgement was acceptable since CR≤ 0.1. We have also discovered that virus (0.412) is the most frequent threat, followed by network failure (0.293), power surge (0.187) and hacking (0.108) is last. The management were recommended to use power suppressor, stabilizer and electrician to monitor power supply, use anti-virus, screen system users and obtained authentic internet garget.***

Keywords: Threat Analysis, Virus, Analytic hierarchy, frequency, consistency ratio and power surge

1. Introduction

An information security may be defined as the process of protecting data from unauthorized usage. Ajibuwa 2008 defined it more explicitly as 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 share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them. These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms.

According to Liag and Xue (2009) Information technology is a double-edged sword. When its power is properly harnessed to serve virtuous purposes, it has tremendous potential to improve human and organizational performance. However, when it is exploited for malicious purposes, it can pose huge threats to individuals, organizations, and society. Many forms of malicious IT such as viruses, worms, e-mail spam, spyware, adware, and Trojan horses can affect personal computers and even enterprise IT infrastructure, causing large-scale productivity and financial losses (Bagchi and Udo 2003; Stafford and Urbaczewski 2004). According to a CSI/FBI survey (Gordon et al. 2006), the 313 participating U.S. organizations lost $52.5 million in 2006 due to computer crime and security problems, of which $15.7 million was caused by virus attacks. The worldwide financial cost of virus attacks in 2006 was $13.3 billion (Computer Economics 2007). Given this gigantic impact, IT security has drawn great attention from researchers and practitioners (Baskerville 1993; Dhillon and Backhouse 2000; Loch et al. 1992; Straub and Welke 1998). To prevent potential harm and losses, a critical IT security issue is that end users need to perform the tasks that are necessary to effectively cope with IT threats. Thus, it is imperative to have a profound understanding of IT users' threat avoidance behavior. Given that safeguarding IT (e.g., anti-virus and anti-spyware software) can reduce the threat of malicious IT, many information systems researchers have applied technology acceptance theories to investigate people's adoption of safeguarding IT. A commonly held belief is that adoption of safeguarding IT is the same as avoidance of malicious IT. This is not surprising given the preponderance of acceptance theories coupled with the very limited reliance on avoidance theories in the IS literature. Actually, it appears quite reasonable to apply acceptance theories in the IT security context because it is important to understand individuals' adoption of safeguarding IT. However, strong theoretical and empirical evidence shows that there are fundamental differences between adoption and avoidance behaviors (Carver and White 1994; Elliot 2006; Elliot and Covington 2001). While studying adoption of safeguarding IT provides some useful findings, this approach tends to draw an incomplete picture of the phenomenon of IT threat avoidance. For example, to avoid a virus spreading through e-mail, users must first perceive the virus as a threat and can take several actions such as enabling a firewall, updating their anti-virus software, or stop checking e-mail. If only adoption of the anti-virus software is studied, we can at best partially understand the avoidance phenomenon because that approach fails to consider the evaluation of threat and alternative avoidance actions. Moreover, in IT security practice, the ultimate goal is to avoid IT threats rather than to adopt a specific safeguarding IT. Adoption of safeguarding IT is only one means that may lead to the goal.

Licensed Under Creative Commons Attribution CC BY

Threat analysis gives how potential adversaries exploit system weakness to achieve their goals. It identifies threats and defines a risk mitigation policy for a specific architecture, functionality and configuration. In a threat analysis security metrics are a challenging requirement in order to determine the status of network security performance and to further enhance it by minimizing exposure to considerable threats and vulnerabilities.

In the more recent years the huge diffusion of new technologies and internet increases the need of security, because communication networks are used to transfer increasingly sensitive information that can be valuable and confidential, requiring protection against human misuse and also attracting attention of malicious people. Network security is the process by which digital information assets are protected, where the word security means protection against attacks by malicious outsiders or insiders. All networks to achieve its fullest potential need to be protected from threats and vulnerabilities. The process to identify the threats, which consists in identifying how potential adversaries exploit system weaknesses to achieve their goals Prasad (2007), and find appropriate countermeasures, is the threat analysis. This process is necessary for specifying a solid and complete set of security requirements so as to build all needed security mechanisms efficiently protecting the system. Moreover, when conducted on an existing system, a correct evaluation of the threats and vulnerabilities allows prioritizing them, assessing the security of the system and proposing an optimal enhancement plan (Duggan and Michalski, 2007)

One of the most valuable benefits of a comprehensive threat analysis is the ability to prioritize security initiatives, including corrective action to address vulnerabilities. Understanding the relative likelihood and impact associated with identified threat sources allows the information security professional to appropriately allocate resources to weaknesses that are more likely to be attacked. Given the limited resources available to most financial institutions, 100% correction of all vulnerabilities is not a feasible option. Accordingly, the knowledge of where attacks are likely to originate, their motivation, and their behavior pattern represents valuable intelligence that can help formulate a targeted information security strategy (Bonnette 2003).

Ibrahim Babangida library of ModibboAdama University of Technology Yola, is facing information security challenges just like other libraries. 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? Hence this study was carried out to address the technological perspective of information security challenges of Ibrahim Babangida Library of ModibboAdama University of Technology, Yola.

2. Methodology

The data for this analysis were obtained from the Ibrahim Babangida Library of ModibboAdama University of Technology, Yola using structured questionnaire and personal interviews. The data were analysed using Analytical Hierarchical Process (AHP) as follows; The technological threats in Ibrahim Babangida Library were rated using Saaty rating scale (1980). Sa'aty's rating scale in Table 1 below was use as a guide to compare the sources of technological threats.

Table 1: 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.

The Technological threats in Ibrahim Babangida Library were categorized into four, namely Power surge (P), Hacking (H), Computer Viruses(V) and Network failure (N) the comparison matrix of the threats is given below

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

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

Where
PH, PV, PN……VN in the matrix above are different ratings of technological threats from standpoint of severity S and frequency F.

The weight of power surge (W_P), hacking (W_H), Virus (W_V) and network failure (W_N) were computed by normalizing and taking the row averages of matrix A .

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

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

Where

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

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

Licensed Under Creative Commons Attribution CC BY

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

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

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

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

Licensed Under Creative Commons Attribution CC BY

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

Licensed Under Creative Commons Attribution CC BY