NETWORK RISK MANAGEMENT

Jamil Asim[1], Umer Shafique[2]
University of Education, Main Campus Okara, Samadpura Road Okara, Pakistan
jamil_asim@msn.com, alex18uk63@yahoo.com

Abstract

Internet has proved a change agent that has re-styled the entire fabrication of Man's life. However, Network Thieves" or "Network Debasers" maneuver to make the mechanics of networking ineffective. The main objective of the present study was to clarify the very concept of Network Security by taking into account the risks in Networking and to suggest measures to avoid these risks. The research confirmed Network Security threats were caused by the Computer's user's carelessness or as a result of lack of awareness about the mechanics of using this magic Machine. The total Population of the study consisted of 100 IT experts of 6 private and public sector universities of Punjab, Pakistan. A close ended questionnaire comprising 20 questions was adopted as the tool of the study. The major findings of this study showed that there were numerous of Network Security risks maneuvered by the "Network Pirates". Network Security can be attained and retained in the Cyber-Scenario by using appropriate "Network Risk Management" Procedures.

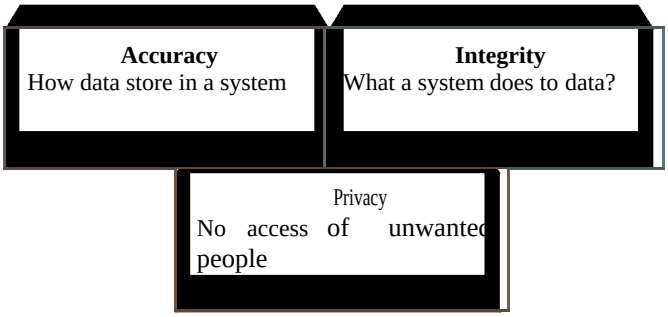
Keywords

Network, Virus, Security, Risks, Computer, Data

Introduction

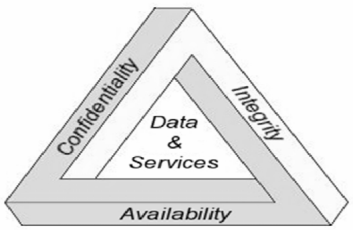
Ours is an N-Gen in Tapscott's phrase. The entire world is at an arm's length, just a click away. Even Aladdin's lamp is no more a fairy-tale phenomenon. In the Modern Jazz world, life without the magic Machine called Computers is a pretty fantasy. Gone are the days when kids used to cuddle against their grannies to listen to the winter-tales of Cindrella, Alibaba and Sindbad. No more are the years when little hands would practice on chisels to master the spellings of their names. Now, as Mubashra Qauddus (2004) puts it "strange words like msn, brb, cya" are in the limelight. The cute wonder-box called computer is actually a Pandora box that has God's plenty to offer. But it seems to be a "Universal Law" with Man to debase and deface any phenomenon that renders benefit to his race; the benefits of internet have also been besmirched. The concept of "Network Risk Management" was introduced to check this mishandling of technology. **Pinkerton** defines Network Security Management as a process that involves "all the sensible steps a management should take to enhance the security of its computer operations". Another technology writer Schneier (2002) considers Computer Security not a technology problem but a people's problem. He presents a "Three Faced Security Model".

Miller (1996) states that Network Security" is about "preventing unauthorized access to a system and its contents". His Model of "Network Risk Management" is:



Solomn and Chapple (2005) presented the following CIA Triad to explain the concept of "Network Security".

.



Cooper's (1989) Model of Six Security Environment is very crucial to comprehending the concept of Network Security.

Network Security	Safety from Viruses, Spasm, Hackers
Personnel Security	Safety of Computer components,
Regulatory Security	Safety provided by the Country Law
Physical Security	Safety from the people within the organization
Hardware Security	Safety of the hardware parts
Software Security	Safety from Piracy of the software

The hazards of Network Security are:

Security Threats	**Description**
Viruses	A parasitic Program infecting the legitimate program
Denial-of- Service	Block the legitimate program.
Data Diddling	Unwanted alterations in data
Encryption	Data turned into gibberish format
Hacking	Interception of keystrokes
Spam	Unwanted interruption,

(Jones, 2001, Norman, 1983, Dr. K., 2000, Roberts 2001, Danish, Mehrassa, Law, 2002 Curtin, 1997, www.crime-research.org , Solomn and Chapple, 2005)

The best protection against these threats is the planning and implementation of security measures. (Jones, 2001, Norman, 1983, Danish, Mehrassa, Law, 2002 Curtin, 1997)

Backup Procedures	Useful in recovering damaged data
Antivirus software packages	These counter most virus threats.
Virtual private networks	Proper configuration and administration of your VPN by Certified Network Administrators.
Identity services	These services help to identify users and control their activities and transactions on the network.
Anti-virus software	Regular scans must also be performed to catch and stop the spread of any virus which does enter your system.
Keep Software Up to-date	Windows, browsers and software must be continuall50y updated.
Computer use policies	Users must be made aware of Security procedures.
Firewalls:	Protect your system and your data from unauthorized access

The present research paper focuses on the Network Security Challenges in the private and public sector universities of Pakistan. In order to obtain an impression of the IT professionals working in the universities of Pakistan, a survey was carried out within the campuses of 6 private and public sector universities of Punjab, Pakistan. These universities include:

1. **University of the Punjab, Lahore**: *the most reputed university of Asia, situated in Punjab , Pakistan. It has the total population of more than 7000 IT professionals.*
2. **University of Education, Okara**: *A public sector ever-expanding university with its sub-campuses situated in the backward areas of Punjab, Pakistan.*
3. **GC University, Lahore**: *A public university with an ever-growing population of IT professionals.*
4. Superior University, Lahore: *A private sector rapidly expanding university, busy in efforts to promote IT education in Pakistan.*
5. **Bahauddin Zakriya University**, Multan: *situated in the backward area of Punjab, Pakistan. This university has carved its niche in promoting IT education in the neglected areas of Pakistan.*
6. **Iqra university, Lahore**, *A private sector university making its presence felt on the scenario of IT development in Pakistan*

This paper reports the results of the survey describing IT expert's opinions about the possible measures for the retention of data on the Magic Machine called Computer.

Objectives of the Study

The objectives of the study were to:

1. Bring to light the Threats to Network Security in the universities of Pakistan
2. Take into account the factors that cause Security Risks to the E-data.
3. Evaluate the impact of Network Piracy over the proper functioning of the organization
4. Suggest measures to minimize Network Security Risks

Significance of the Study

The present Research is very important for those who are interested to find some way out of the destructive Network Theft. The present Research is very important for those who are interested to find some way out of the destructive Network Theft. This will prove immensely beneficial for the computer personnel as it would suggest to them how they can save their hardly – compiled data be gone to dogs in just micro-seconds. The Computer Crimes Investigation Institutions and FBI can rely on this study to measure the magnitude of

Network Security Risks prevailing in Pakistan. This study may also prove useful in setting work-targets and Action-plans for the Information Ministry of the Government of Pakistan as the manifesto of this study is "Say No to E-Security Threats" On a more specific level, this study is useful for the university level high ups as data retention measures in this study would save them from colossal data losses resulting in heavy financial setbacks. Also this study will be significant future researchers as it would open fresh vistas of knowledge in the Science of E-Data Retention

Assumptions of the Study

The research was based on the following assumptions:

1. Computer data in Pakistani universities is ever exposed to certain severe Security Risks.
2. Network Security problem is the offshoot of the Computer User's carelessness
3. Most of the Computer personnel in Pakistani universities were unaware of the E-Confidentiality Mechanism.
4. Safeguarding measures taken against Network Security Risks are not used properly.

Methodology

This paper reports on one phase of a Survey which was conducted on the computer professionals working in Pakistani Universities. The study was delimited to Punjab Province only. The computer professionals in the 23 Public and private universities of Punjab ranged up to 12000 in number. Only 100 computer professionals from 6 out of 23 public and private sector universities were selected as the sample of the study. The sample was drawn using proportionate sampling technique and the proportion from each university was as follows:

Name of the University	**Approximate Population of IT Professionals**	**Number of the Elements selected from each university**
University of the Punjab, Lahore	150	30
University of Education, Okara	20	10
GC , University , Lahore	100	25
Superior University	15	05
Bahauddin Zakria University Multan	100	25
Iqra University , Lahore	15	05
Total	**400**	**100**

A close ended three -part questionnaire comprising 20 questions was adopted as the tool of the study. The Questionnaire was framed around the respondents' experiences to tackle with Network Security Threats.

Section I of the Questionnaire contained open ended queries about the IT Professional's awareness of Network Risk Management; i.e. their definition of Network Risk Management, their knowledge about different Security threats and their common practices on their systems.

Section II of the Questionnaire was Scenario-based. It inquired about how many times in a month the Network Threats attacked on computers, what type of damage they rendered and how much hazardous they were for the Organization.

Section III of the Questionnaire contained several close ended questions about which Network Risk Management Procedures are being used in the universities of Pakistan.

This questionnaire was distributed in 100 IT experts of the 06 universities of Punjab, Pakistan. Participation was both anonymous and voluntary. Since the researcher gathered the data personally, the Return- Ratio was 100%. All the respondents were co-operative in filling out the questionnaire as they themselves were the staff members of the Organizations in question.

Results

100 IT experts participated in this survey participated in the survey with 100 usable responses corresponding to a 100% response rate. The respondents ranged in age from 21 to 54 with a mean of 28.4 (SD = 7.79). There were 75% male and 25% female. *IT experts' Concept about Network Risk Management*

The IT experts were not clear about the concept of Network Risk Management. They simply took the attack of Viruses as Network Security Risk. 89% of the respondents hardly knew that Denial of Service was a Network Security Risk. They simply took it to be a "Server Problem". 76% of the respondents were not aware of the fact that the data once encrypted can hardly be corrected. 98% of the respondents reported that they did not bother to construct a strong password on computers. 54% clicked to spam invitations on their systems. 67% reported that they ignored Network Security updates because of their pre-occupation with office work.

Recurrence of Network Security Threats in the Universities of Pakistan

All the respondents (100%) reported that they often have to go through the destruction, diddling or encryption of their hardly compiled data. 78% respondents reported that they had to suffer from economical loss as a result of Network Security hazards. 100% of the respondents opined that they underwent worst kind of nervous strain when their data is hacked. 77% of the respondents reported that their data was hacked. 100% of the respondents that their systems were attacked by Network Security threats like Viruses etc. on daily basis. 100% of the respondents termed Viruses to be a great deterrence in their office work. 77% of the respondents complained denial of service on their systems at least thrice in a day.

Network Risk Management Procedures

87% of the respondents opined that they prepared backups of their files. 100% of the respondents have installed Virus scans

on their computers. 73% of the respondents have installed encryption software on their computers. 78% said that they often forgot to scan their computers for Viruses. 83% reported that they remembered to scan their computer only if it is infected. The recommendations that the respondents made for E-data security were to:

1. Avoid Network Threats,
2. Ensure backups,
3. Avoid systems with single points of failure,
4. Stay current with relevant operating system patches,
5. Watch for relevant security advisories, and
6. Install Antivirus software packages.
7. Firewalls (software and/or hardware)
8. Anti-virus software/Anti-adware/Encryption software

Discussion

In the results section of the paper, the results are summarized and described. In the discussion section, they should be interpreted, critically evaluated, and compared to other reports. The IT experts' answers to these questions rendered a valuable lot of quantitative data reporting that 100% of the respondents faced Network risks on their workplace desktops. 87% of the respondents were of the view that Data Loss on computers is the offspring of the users' carelessness or lack of awareness about using the Computer. Only 33% opined that Data Loss occurs not because of the users' carelessness or lack of awareness about using the Computer. Only 33% opined that Data Loss occurs not because of the users' carelessness or lack of awareness about using the Computer but because of the filthy maneuver of the Data Debasers. All the respondents were of the view that Network Security Risks can be minimized if E-safety measures are adopted to throw a gauntlet to these Risks. The results will be discussed keeping in view the basic assumptions of the study.

Assumption 1: Computer data is ever exposed to certain severe Security Risks.

Amongst the sample, 100% of the respondents reported to suffer at the hands of Network Security threats. This number indicates how much Cyber-Scenario in Pakistan is prone to Network threats. The result on this assumption outdoes the FBI-CSI Survey (2005) which mentions that security measures in the 67% of the organizations are outsourced.

Assumption 2: Network Security problem is the offshoot of the Computer User's carelessness

The research data brought forward confirms this assumption. Large majority of the respondents were found careless or ignorant about the mechanics of using the Machine.

Assumption 3: Most of the Computer personnel in Pakistani universities were unaware of the E-Confidentiality Mechanism.

Large majority of the selected sample were unaware of the E-confidentiality mechanism. 78% of the respondents said that they often forgot to scan their computers for Viruses.

Assumption 4: Safeguarding measures that are taken against Network Security Risks are not used properly.

The results show that the IT experts of universities of Pakistan are careless about using Safeguarding measures against Network Security Risks. They are negligent towards the proper use of Virus scans and they hardly pay diligent attention towards scanning the systems at all.

IMPLICATIONS OF THE UNIVERSITY

In the light of the Discussions made above, following suggestions can be put forward to avoid the Networking threats in the universities of Pakistan.

1. IT personnel must be trained well in E-Confident laity Policies and in the appropriate use of Computer Scan system.
2. A legal Plan must be envisaged to throw a gauntlet to E-Security issues.
3. Seminars and Research Symposiums must be conducted to create awareness about "Network Risk Management".
4. A holistic plan for Computer Security must be formatted.
5. The technical assistance of foreign qualified staff must be sought after to envisage a fool-proof Security System for the universities of Pakistan.
6. The services of Security advisors must be hired and their must be Support Personnel working round the clock to listen to the complaints of the IT staff.
7. IT staff must be taught to discourage if somebody uses their system without their permission.
8. All the universities of Pakistan must put forward the suggestion to the government that a law against Network Damage must be passed.

Conclusion

None of these approaches alone will be sufficient to protect a network, but when they are layered together; they can be highly effective in keeping a network safe from attacks and other threats to security. In addition, well-thought-out corporate policies are critical to determine and control access to various parts of the network.

REFERENCES

1) Article on Network Security retrieved from http://www.esecuritytogo.com/ccpage.aspx dated 12-12-2008
2) Cooper, J.A. (1989) Computer and communications security: strategies for the 1990s: McGraw-Hill: New York
3) *CSI/FBI Computer Crime and Security Survey* (2005) retrieved from www.gocsi.com dated 12-03-2009
4) Curtin, M.(1997) *Introduction to Network Security* available at www.interhack.net
5) Danish, A., Mehrassa, & Law, F. (2002) *Safe and Secure: Secure Your Home Network and Protect Your Privacy Online*: SANS Publications USA
6) Jones, D. (2001) *How to Do Everything with the Internet:* McGraw-Hill Companies Limited. New York

7) K, Dr. (2000) *A Complete Hacker's Handbook*. CARLTON Books New York:
8) Miller, S.E. *Civilizing Cyberspace*: ACM Press USA: (1996)
9) Mubashra Qauddus (2004) Newspaper article: Dawn, (Pakistan)
10) Norman, A. (1983) *Computer Insecurity:* Chapman & Hall: New York
11) Norton, P. (1998) *Essential Computers* (5th Edn) New York: Glencoe
12) Roberts, S. Fiet, M. Bly, R.Y (2001) *Internet Direct Mail: the Complete Guide to E-Mail Marketing Campaigns*, NTC / Contemporary Publishing Group Chicago:
13) Schneier, B. *Counterpane and Managed Security Monitoring* available on www.counterpane.com (2002)
14) Solomon, M.G. & Chapple, M. *Information Security Illuminated* Singapore: Jones and Bartlett Publishers: USA: (2005)
15) Tapscott, D. (1998) *Growing up Digital*: McGraHill Companies Limited. New York
16) Webber, J (1985) *Tomorrow's World Computers: the Next Generation*. ARCO Publishing Inc. New York: