Network Security and User Awareness in IT Organisations

S.Sathiyaseelan and P.Filmore

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

It is obvious that in today’s internet world not only the internet users are increasing in number but also the security threats. To protect the network from getting attacked, the security level and the awareness level of the users must be improved to a sufficient level. This research entitled ‘Network Security and User Awareness in IT Organisations’ aims at analysing the current network security level and level of user awareness in IT organisations. This research is conducted in the form of a survey in which the questions were focussed on the topics namely, security level and security breaches, security trends and methods, security policies, management issues on security.

The questionnaire comprised of 25 questions among which three of the questions were set to be compulsory. Seventy four responses were obtained from seven of the IT organisations. As the questionnaire comprised of less number of compulsory questions, the chance given for the users to skip the questions of concerned in retrospect. From the analysis, recommendations were developed for the users regarding how to handle security issues and how to improve security level in IT organisations.

Keywords

Network security, questionnaire research, security breaches, security trends and methods, security policy, management issues on security.

1 Introduction

The computer users and the usage of the internet are increasing day by day. Computers communicate with each other by the means of a network. The expansion of a network can be restricted within a small building or it may cover a wide area also (Davies and Price, 1984). Not only is the internet usage increasing rapidly but also the crimes on the other hand (Maiwald, 2003). These crimes are happening due to the network vulnerabilities and also due to the user’s unawareness in the field of network security (Canavan, 2001). The computer hackers are (Stallings, 2000) creating threats to the computers and vulnerability attacks to the computer network. Lot of laws have been (Devargas, 1993) created by the government to punish the hackers. Implementing these laws alone cannot serve as the best way to reduce the cyber crimes.

Nowadays we are coming across lots of news about the network security attacks by the attackers in newspapers and internet Devargas, 1993). The attackers not only target the private organisations but also target the Department of Defence (DOD) and other government organisations (Devargas, 1993). The attackers either steal or destroy the confidential data of the organisations. They attack the social networking web sites and the most famous commercial web sites such as Yahoo, Amazon, eBay, etc. It is not necessary that the attacker must be external attackers. There are many internal attackers such as employees or former employees of an organisation who attempt to steal the organisation's salary information or important data (Maiwald, 2003). All organisations are monitoring (Canavan, 2001) their own network to prevent unauthorised intrusion and other types of attacks. Every organisation spends a lot of money on network security. Improving awareness of network security among computer users plays a main role to reduce the cyber crimes.

2 Need for Network Security

With a rapid increase in the number of corporate networks, there has been an increase in the bandwidth over the internet. Internet has been put to use for communication purpose, remote connection to the corporate network and also for commercial transaction in recent days (Devargas, 1993). As there has been an increase in the uses of the internet, the number of threats being posed by the hackers are also increasing day-by-day. Due to these threats like spam, phishing, etc., the customer distrusts the corporate companies and organisations for online transaction. As a result, the companies face some amount of loss (Bhatnagar, 2002). There are network security tools and network security policies (CISCO Systems, 1992) to protect the network or computer systems. The network security prevents the unauthorized users to access the network, thereby securing the company's network and otherwise making the organisation as a reliable organisation.

3 Network Security Threats

Any disorder that affects the normal activity of an individual system or the entire network, like affecting the integrity, functionality of the system intentionally or naturally can be defined as threats (Canavan, 2001). Threats that causing damage or loss are classified into following three types (Devargas, 1993), they are active or passive threats, logical or physical threats and deliberate or accidental threats.

4 Methodology

The main purpose of this research is to collect the information based on the questionnaire, understanding the information and processing those obtained information to write recommendations for the IT organisations. This research consists of different types of questions and quantitative methodology.

4.1 Development of questionnaire

4.1.1 Analysis of previous research

Previous research is analysed under the heading ‘Network security and user awareness’. The reports of previous research that undertaken is collected and analysed.

4.1.2 Analysis of previous data collection method and create own research methods

The previous data collection method for the previous researches is analysed. Then our own questionnaire is created for the quantitative research method depending on the research. Then that obtained research method is implemented to collect data.

4.1.3 Trial Implementation of Questionnaires

A trial questionnaire is implemented and it is tested by using the Survey monkey website with suggestion of my project supervisor. Then the URL link of the survey is sent to Plymouth University students by email with permission of my project supervisor. After testing the questionnaire, the reports are collected from the students and analysed. The mistakes are corrected which have been done in the trial questionnaire with the help of observed reports. Specific changes are included in the questionnaire.

4.1.4 Implementation of Questionnaire

The questionnaire is implemented for computer users in IT organisations. The expected minimum respondents are 70 and maximum respondents are 100 for this research. Then the reports from the computer users are collected and analysed.

4.1.5 Analysis of collected data from the reports

The data is collected from the computer users in the IT organizations are documented properly. After collecting the data, the results obtained are analysed and recommendations are then developed. After this process a conclusion of each part of the research is made and a final report is created.

5 Analysis Summary

From this research analysis of the questionnaire it has been observed that 52.4% of the respondents in the IT organisation have some awareness of the technologies and methods being used in their IT organisation. 5.92% of the respondents have commented about the antivirus and firewall used in their IT organisation. It proves that they have some knowledge about network security in their IT organisation. The other 48.6% of respondents do not possess sufficient knowledge regarding the network security methods used in their IT organisation. So it is clear that the computer users need more training regarding the network security and the organisations are responsible for making the computer users aware by providing proper copies of policies and proper security training.

6 Recommendations:

The recommendations are based on the analysis of the results obtained from the questionnaire and the background research. The recommendations are divided into five parts, based on the questionnaire. The five parts are security level and breaches in organisation, security trends and methods in organisation, security policies in organisation, management issues on security in an organisation and issues improving organisation's security level.

6.1 Security level and security breaches

From this research it could be observed that most of the organisations do not show much interest in network security. The security level of the organisations is in an average level (43.20%). **Recommendation:** *The organisation should be aware of network security. The respondents also should cooperate with the organisation to improve their network security from security breaches.*

The results obtained from the research show that 35.10% of the organisations have suffered from Malware and from other types of malicious threats. These types of threats are occurring due to vulnerability in the network and unawareness of respondent on network security in their organisation. This research paper analysed that 28.35% of the organisation have the highest security risk on internet downloads. **Recommendation:** *This is the responsibility of the organisation to improve their security level by implementing proper security mechanisms and tools. The respondents should improve their awareness on network security to prevent themselves and their organisation from these types of malicious threats.*

6.2 Security trends and methods in organisation

This analysis observed that 66.20% of the organisations have secure backup disk for important data and 32.45% of the organisation are not having that secure backup disk. **Recommendation:** *Every organisation must have secure backup disk for important data.* Nowadays most of the employees are using portable devices for communicating with the organisation's network. Some of the employees are working from their home and access the organisation's network. **Recommendation:** *Wi Fi protected access and end point security should be implemented for secure access of organisation's network.*

The research observed that only 48.60% of the organisations are currently using automated patch management and vulnerability scanner. Recommendation: The respondents and the security administrator in the organisation should be aware of implementing the automated patch management and vulnerability scanner in their systems to in order to prevent the attacks from occurring.

It was found out from the research that 30.72% of the organisations are using both antivirus and firewall. 36.42% of the organisations are using Kaspersky antivirus and Norman personal firewall. 18.45% of the organisations are not using either the spam control or the anti spyware. **Recommendation:** *Organisations should implement all types of security mechanisms such as antivirus, firewall, spam control, antispyware, etc., in order to improve their network security level. The respondents and security administrators should be given training and made aware of implementing the security tools in their organisation.*

This research observed that 44.55% of the respondents are interested in using the password authentication technology mainly because of the reason that it is cost effective. 39.15% of the users have felt more comfortable in using the biometric technology because of its enhanced performance. **Recommendation:** *It is suggested that the organisations should implement password authentication and biometric technologies to prevent the IT organisation from security breaches such as identity theft, data loss, etc. The employee must be made aware of the technologies that have been used in their organisation.*

6.3 Security policies in organisation

This research observed that 74.25% of the organisations have network security policy, password policy and some of the organisations are also have a security team. 24.30% of the organisations do not have them. **Recommendation:** *It is very essential that all of the IT organisations must have the policies and also a security team to update those security policies regularly. These policies must be updated frequently based on the security breaches that the organisation is expected to face, so that the organisation could be saved before the attacks have occurred.*

This research observed that 75.60% of the organisations have provided the security policies implemented in their organisation to the respondents. But 21.60% of the organisations have not provided the network security policies implemented to respondents. There is no purpose in creating network policies without them being implemented. From this conducted research it could be observed that only 58.10% of the organisations provide security training to the respondents in their organisations. **Recommendation:** *It is suggested that security training must be provided by the organisations to all of the respondents in their organisations. The respondents should also follow the security policies and security training given in their organisation to protect their systems and network from malicious attacks.*

6.4 Management issues on security in organisation

This research observed that 51.30% of the organisations are spending 11-30% of organisation’s IT budget for security. 64.80% of the respondents accept that this budget is enough to cover their security requirements of the organisation and 32.40% of them do suggest that it is not sufficient enough for their organisation. 63.45% of the respondents assure that it is possible for them to convince their organisation’s management to invest more amounts in security solutions. **Recommendation:** *The respondents have the best opportunity to convince the organisation’s management to make more investment on security requirements. So it is suggested that the* *respondents must use the opportunity to convince the organisation's management about the implementation of the security equipments.*

6.5 Issues to improve organisation's security level

It could be observed from the research that 48.60% of the respondents accept that better awareness on security among employees help to improve the level of security in the organisation. **Recommendation:** *The major issue that helps to improve organisation's security level is the level of awareness of the computer users regarding the security issues. So IT organisation management and employees should cooperate to improve the security awareness level among computer users.*

7 Future Work

As all of the questions were not made compulsory, many of the users used their chance to skip the questions, which could be stated as a very important limitation of the research. In order to avoid this issue and extend the research, future researchers may conduct the same research with all of the questions made compulsory, which will improve the level of analysis.

In this research, the responses have been collected from the employees of the IT organisations. But their role in the IT organisation was not determined. Future researchers may add some extra questions in the research covering the aspects such as the role of the employee in the IT organisation, number of employees in the organisation and the security training methods implemented in the organisation. This will deepen the analysis of the further.

This research was conducted using quantitative methodology, future researchers may conduct the same research using qualitative methodology, which will provide more details for analysis and as a result further better recommendations could be provided.

8 Conclusion

There is a rapid increase in network and also new networking technologies every day. There are lot of challenges that the networks in IT organisations and in other enterprises should face. The new security technologies are also arising everyday to encounter these challenges. In any IT organisation, security is a major issue to protect their network and data. The computer users are considered to be the backbone of an IT organisation. This research is has tried to analyse the awareness level of the computer users in an IT organisation regarding the network security and its tools.

This research analyses in deep the issues such as the security solutions and mechanisms implemented in the IT organisations to protect their own network, security threats to the organisation, security policies and organisation's IT budget to security. These issues are related to the security awareness level of in the IT organisations. The results obtained from this research show that the computer users in IT organisations are having some level of awareness on network security and security methods implemented in the IT organisations. But they do not have a very good level of awareness on the network security and security solutions implemented in their organisation. It seems that IT organisations are not concentrating more on improving the awareness level of the computer users in their organisations. When the users are not given appropriate training they may remain unaware and as a result, they may open the door for the hackers to enter into the secured network of the organisation.

This research has recommended that the IT organisations should improve the awareness level of network security among computer users in their organisation by implementing the network security policy in their organisation and also by providing proper security training to the computer users. The organisation should accept and provide the requested network security requirements of the computer users in the IT organisation. The computer users should follow the security policies and security training given by their IT organisation. The computer users should also have a sufficient level of awareness on network security methods used in the organisation.

9 References

Bhatnagar, K. (2002) Cisco security, Ohio: Premier, ISBN: 1931841845.

Canavan, J.E. (2001) Fundamentals of Network Security, Artech House, London.

Cisco Systems Website, (1992) ‘What Is Network Security?’ http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/secure_my_business/what_is_network_security/index.html, (Accessed 24 June 2010)

Devargas, M. (1993) Network security, Oxford: NCC Blackwell, ISBN: 1855542013.

Maiwald, E. (2003) Network security: a beginner’s guide, California: McGraw Hill, ISBN: 0072229578.

Stallings, W. (2000) Network security essentials: application and standards, New Jersey: Prentice- Hall, ISBN: 0130160938.