

The Future of Organization's Computer Network Security for the Next 5 Years (2011-2015) by Using Delphi Technique

Cholatip Yawut⁺ and Phattarapong Keawpipop

Faculty of Information Technology

King Mongkut's University of Technology North Bangkok, Bangkok, Thailand

Abstract. Security is one of the important factors in an organization's computer network because the network connects to other networks through the internet. An attack on the organization's computer network can be possible from outside of the organization. Therefore, computer network security is very important to prevent and protect the organization from internal and external attacks. The purpose of this research is to predict the future of computer network security for the next 5 years (2011-2015) by using Delphi technique which is a widely used and accepted method for achieving convergence of opinion concerning real-world knowledge solicited from experts within certain topic areas. The research result can be used to ameliorate and develop organization's computer network security including staff, hardware, software and privacy system.

Keywords: Network, Security, Trend, Delphi Technique

1. Introduction

In the past several years, most organizations have created a computer network and use it daily. It is called a local network which provides the access service for members of the organization. An important application running on the network is the Intranet which links all users in the organization to collaborate. Moreover, schedule of work in a team called the Workgroup plays an important role; each team has their own information system and station information services called the server. Working in the workgroup level aims to join the specified groups such as team of sales, accounting, finance, manufacturing, etc. Intranet includes these groups together as an organization's private network used to exchange and share information which we call a network workflow. However, the scope of the network is not only within the organization. Nearly all organizations join their intranet accessing to the Internet to collaborate with other organizations which is a way of improving performance, speed and comfortable works. Many organizations have their own web site to promote their products and services. The orders from outside or providing after sales services will be received or sent directly through the network.

Currently, many computer users mistakenly think that a firewall can protect 100% of the network system, but in fact, the firewall alone is insufficient [1]. For example, an administrator sets up the firewall rules to block access to the web server ports by allowing connection on port 80. It can prevent the network when a hacker tries to attack ports 139 or 445. But if a hacker tries to attack the web application using port 80 and if the vulnerabilities exist, the hacker can then attack the web server without any warning issued by the firewall. Therefore, an IDS (Intrusion Detection System) is proposed as an alarm system. It will give an alert when it detects someone attempting to attack the computer network. Another IDS calling IPDS (Intrusion Detection Prevention System) or IDP (Intrusion Detection and Prevention) is a device used to simultaneously detect multiple network attacks by detecting the traffic passing through the network and analyzing it.

This research uses the Delphi Technique [2-7], a scientific method to gather information from a group of experts, many people attempt to study and analyze the knowledge to forecast the future in various fields, especially science. Science and technology are continually changing all the time. Research with the Delphi technique is regarded as future science (Futurism), focusing in-depth research to provide knowledge and better understanding about the future. Besides, it can warn the user of unforeseen things which can happen in

⁺ Corresponding author. Tel.: + 6629132500ext2728; fax: +6629122019.
E-mail address: cholatipy@kmutnb.ac.th.

the future. The purpose of future research is to forecast the expected future which we can seek ways to prepare control and improve to meet future needs. In this study, the Delphi Technique is used to predict the future trends of organization's network security for the next 5 years (2011-2015). This research utilizes questionnaires to survey the opinions of security experts in organization's network security.

In the rest of the paper, we describe related works in section 2, explain research methodology in section 3 consisting of research procedure and questionnaires, explain the research results in section 4 indicating organization's computer network security in today's market and for the next 5 Years, and summarization in section 5.

2. Related Works

The Delphi technique [7], mainly developed in the 1950s, is a widely used and accepted method for achieving convergence of opinion concerning real-world knowledge solicited from experts within certain topic areas. Predicated on the rationale that, "two heads are better than one, or...n heads are better than one", the Delphi technique is designed as a group communication process that aims at conducting detailed examinations and discussions of a specific issue for the purpose of goal setting, policy investigation, or predicting the occurrence of future events. Common surveys try to identify "what is," whereas the Delphi technique attempts to address "what could/should be".

Network security [8] consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources.

[9] indicated that the network security should focus more on the process rather than the network device to achieve a highly secure organization's network.

[10] stated that the one thing most valuable to the organization is data or information, so protecting the data or information is very important and necessary in the information age. In this era, who possesses more information has the advantage. Therefore, if the information is hacked or cannot be accessed; it will surely affect the owner. Information stored in the system is vulnerable to attack from multiple sources, so an information system is essential and needs a security system which is robust enough to cope with various threats.

[11] said that current computer systems and network play an important role in everyday life; using the database via a network or via the web browser or accessing to various information systems via the corporate network connected to the Internet. In addition, the network is also needed to run their businesses, whether used to support business operations or conducting business on the network. Security of data or network is very important to avoid loss of data or significant resources.

[2] used the Delphi technique in designing and applying applications. Proving the Delphi technique is a popular and efficient tool identifying and ranking of the important issues for management decision research. However, studies over the past few years have not used the Delphi technique which requires rigid rules for the process of selecting appropriate experts and the principle detailed for the selection.

[3] utilized the Delphi technique for graduate research which stated that the Delphi method is an interesting means for graduate students earning a master's and Ph.D. because it is very flexible and can be used to successfully carry out research.

Referring to prior research, we selected the Delphi method to investigate the future of organization's network security for the next 5 years (2011-2015).

3. Research methodology

The research methodology steps are depicted in the Fig 1. The Delphi technique is utilized to research the organization's computer network security for the next 5 years. We started by studying and collecting information about computer network security and about the Delphi technique. The next step is conducted as the follows.

3.1. Research Procedure

This research focuses on future trends of organization’s computer network security for the next 5 years (2011-2015) by using the Delphi technique. The future trend includes bringing together the opinions of experts in organization’s computer network security by statistical approach. The research methodology uses the Delphi technique which is a research form to study future trends with experts who can provide valuable and reliable information. Three rounds of questionnaire are carried out as described in section 3.2..

Qualifications of the experts, these people have good knowledge, well-known, experienced in computer network security for at least 5 years. Each expert will answer 3 rounds of the questionnaires.

We selected 17 experts on organization’s computer network security as a research sample group divided into two groups;

1. Eight experts from government agencies and state enterprise
2. Nine experts from private enterprise

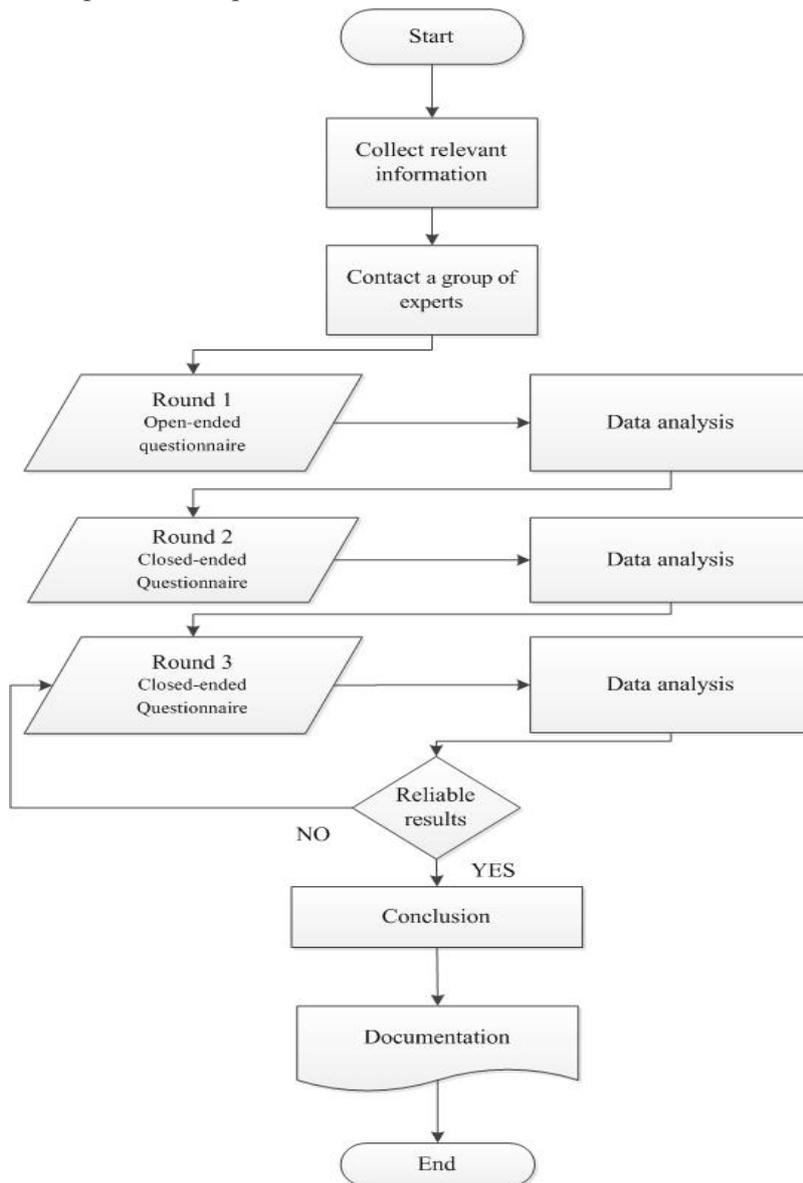


Fig. 1: Research procedure.

3.2. Questionnaires

In this section, we develop questionnaires used as a research tool which is divided into the following three steps:

In the first questionnaire processing, we launched the open-ended questionnaire on the first round to open the issue of potential organization’s computer network security for the next 5 years (2011-2015). The questionnaire is divided into two sections consisting of the first section which asked about the issue of

organization's computer network security in today's market and the second section which surveyed the issue of organization's computer network security for the next 5 years (2011-2015).

Next, we extract the data from the first round questionnaire by evaluating the trend of the questionnaire answers of each expert whether they replied in the same direction. If so, the questionnaire item would be included in the closed-ended questionnaire. Experts, then, rated the questionnaire statement based on a five point scale consisting of "5: strongly agree", "4: agree", "3: not sure", "2: disagree" and "1: strongly disagree" to find common opinion among the experts. We then calculate the value of the median, mode and ranges between the quartile.

Afterwards, the third round questionnaire will also be a closed-ended questionnaire used to select the answers of the experts with a five-point scale which is the same definition as in the second round questionnaire but adding the value of the median and ranges between the quartile. The purpose of this is to have the experts group compare and confirm their opinions in the second round questionnaire. The data processing gives the ranges between 0-1 quartile indicating the result accuracy which led to the final processing to conclude the results.

4. Research Results

The research results can be summarized as follows:

4.1. Organization's Computer Network Security in Today

Nowadays, each organization focuses on technology rather than process or policy of the security management of a computer network within an organization. As a result, the network security is ineffective. Most organizations are careless of managing staff responsible for the organization's computer network security. So, people in the organization have not fully cooperated with the security rules. Therefore, organization's computer network security is inefficient and ineffective. Computer network security can prevent harm at a certain level, but not enough and should be improved in many other parts in the future. The price of equipment used in the network security is also too high. Hence, it is difficult to manage the budget and resource estimation. Some executives may be reluctant to install network security devices due to the high cost whether they focus on computer network security within the organization or not. Each organization will normally focus on the computer network performance rather than the computer network security within the organization. The right picture of computer network security depends on the ability of the staff who are responsible for the computer network within the organization. There are no staff who especially act on computer network security within the organization. The separation of duties, understanding, and the decision of the responsible staff is confusing. As a result, the organization's computer network security is currently ineffective today.

4.2. The Future of Organization's Computer Network Security in The Next 5 Years

An organization's computer network security should have clear policies and penalties. Moreover, it should be strictly enforced by all staff within the organization. Having a widely accepted standard can be used to verify the computer network security.

Persons acting on organization's computer network security should be knowledgeable to perform their duties, and are certified by the knowledge tests about the computer network security from the global security standard organization.

Devices acting on the network and the organization's computer network security should have high performance and be reasonably price. Besides, it should support the centralization management, which can be centrally controlled and processed, including real-time inspection and effectively compatible with other devices. It should also verify real-time unusual movements of the logging, or text on the various systems or equipment and support for any security protocols concerning organization's computer network security.

Software acting on the organization's computer network security and the software running on the network should be able to verify their operation and support for the organization's computer network security, compatible with any software or devices that serve the computer's network security. It should also

support the central management system and always improve their efficiency at a high level and be up-to-date. Besides, the hardware should be at a reasonable price.

The effectiveness of the privacy system in the organization should include single sign-on (SSO) and include high performances; stable, quick and safe. Last but not least, it should be accordance with the computer laws and always up-to-date.

5. Conclusion

In this research, we use the Delphi technique to predict the future of organization's computer network security for the next 5 years (2011). The questionnaires were 3 rounds including open-ended questionnaire and closed-ended questionnaire which were used to collect the opinions from a group of experts. The results illustrate the security of an organization's computer network today and for the next 5 years (2011-2015). To summarize, results indicated the significance of staff, hardware, software and privacy which are all important to anyone who is concerned about network security. This will provide the ability to manage and control the relevant aspects to meet the future needs and security issues of an organization's computer network.

6. Acknowledgements

We would like to thank the experts on organization's computer network security who dedicated their valuable time to answer the questionnaires and give important suggestions.

7. References

- [1] CERT[®] Coordination Center, Home Computer Security. Software Engineering Institute Carnegie Mellon, November 22, 2002. Retrieved March 25, 2011 from <http://www.cert.org/homeusers/HomeComputerSecurity/>.
- [2] C. Okoli and S. D. Pawlowski. The Delphi method as a research tool: an example design considerations and applications, *Department of Information Systems and Decision Sciences*, Louisiana State University, Baton Rouge, LA, USA, 2000.
- [3] G. J. Skulmoski, F. T. Hartman and J. Krahn. The Delphi Method for Graduate Research. *Journal of Information Technology Education*, Volume 6, 2007.
- [4] M. Tiantong. Delphi Technique. *Faculty of Information Technology, King Mongkut's University of Technology North Bangkok*, Retrieved March 25, 2011 from <http://it.kmutnb.ac.th/monchai>.
- [5] Delphi Technique [Electronic version], Retrieved March 25, 2011 from <http://202.143.130.99/files/Delphi3.pdf>.
- [6] H. A. Linstone and M. Turoff. Delphi Method: Techniques and Applications [Electronic version], 2002, Retrieved March 25, 2011 from <http://is.njit.edu/pubs/delphibook/delphibook.pdf>.
- [7] C. C. Hsu and A. Brian. The Delphi Technique: Making Sense Of Consensus. *Practical Assessment, Research & Evaluation* Volume 12, Number 10, August 2007, ISSN 1531-7714. Retrieved March 25, 2011 from <http://pareonline.net/pdf/v12n10.pdf>.
- [8] Network security, *Wikipedia*, Retrieved March 25, 2011 from http://en.wikipedia.org/wiki/Network_security.
- [9] S. Dixit and P. K. Jha. Network Security: It is a process, not product. *SD Bansal College of Technology*, India, 2009.
- [10] C. Pangchan. Master in security. *Info Press*, Bangkok, 2008.
- [11] T. Chomsri. Computer Network Security. *Pro Vision*, Bangkok 2010.