Scientific Research Publishing

Journal of Information Security, 2017, 8, 166-173
http://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Using the Analytical Hierarchy Process Model in the Prioritization of Information Assurance Defense In-Depth Measures?—A Quantitative Study

Rodney Alexander

Hutchinson Community College, Hutchinson, USA
Email: rdnyalex@aol.com

How to cite this paper: Alexander, R. (2017) Using the Analytical Hierarchy Process Model in the Prioritization of Information Assurance Defense In-Depth Measures?—A Quantitative Study. *Journal of Information Security*, **8**, 166-173.
https://doi.org/10.4236/jis.2017.83011

Received: May 20, 2017
Accepted: July 3, 2017
Published: July 6, 2017

Abstract

Organizational computing devices are increasingly becoming targets of cyber-attacks, and organizations have become dependent on the safety and security of their computer networks and their organizational computing devices. Business and government often use defense in-depth information assurance measures such as firewalls, intrusion detection systems, and password procedures across their enterprises to plan strategically and manage IT security risks. This quantitative study explores whether the analytical hierarchy process (AHP) model can be effectively applied to the prioritization of information assurance defense in-depth measures. In response to these threats, the President, legislators, experts, and others have characterized cyber security as a pressing national security issue. The methods used in this study consisted of emailing study participants a survey requesting that they prioritize five defense in-depth information assurance measures, anti-virus, intrusion detection, password, smart-cards, and encryption, with a range of responses from 1 - 5 using a Likert scale to consider standard cost, effectiveness, and perceived ease of use in terms of protection of organizational computing devices. The measures were then weighted, based on ranking. A pair-wise comparison of each of the five measures is then made using AHP to determine whether the Likert scale and the AHP model could be effectively applied to the prioritization of information assurance measures to protect organizational computing devices. The findings of the research reject the H_0 null hypothesis that AHP does not affect the relationship between the information technology analysts' prioritization of five defense in-depth dependent variables and the independent variables of cost, ease of use, and effectiveness in protecting organizational devices against cyber-attacks.

Keywords

Information Assurance, Analytical Hierarchy Process, Defense in Depth, Information Technology

1. Introduction

Organizations have become dependent on the safety and security of their computer networks and their organizational computing devices. However, organizational computing devices such as desktops, notebooks, and smart phones are increasingly becoming targets of cyber-attacks. Information technology (IT) has evolved into its own industry with global networks of interconnectivity, such as the internet.

The field of information security has developed, along with security devices such as firewalls, intrusion detection systems, and password procedures. These devices and procedures are designed to help protect organizations from the misuse and abuse that have developed along with interconnectivity and the internet. As such, business and government often use defense in-depth information assurance measures across their enterprises to plan strategically and manage IT security risks. This research study explores whether the analytical hierarchy process (AHP) model can be effectively applied to the prioritization of information assurance defense in-depth measures.

Scholar-practitioners may be interested in this research because, according to [1], cyber threats pose a significant risk to economic and national security. In response to these threats, the President, legislators, experts, and others have characterized cyber security, or measures taken to protect a computer or computer system against unauthorized access or attack, as a pressing national security issue. There is a question of whether conventional information assurance (IA) process guidance and practice, even if substantially reformed, can adequately respond to the recurrent problems and contemporary challenges of cyber-attacks [2].

Organizational computing devices are increasingly becoming targets of cyber-attacks. The organizational computing device security topic is of interest to practitioners since reporting useful findings is an important part of IT security research. Integrating relevant theory and research into IT security is also critical. According to [3], one of the most dominant applications used by organizational computing devices is the e-mail delivery service.

Theoretical/Conceptual Framework

The best method to describe the theoretical/conceptual framework is to picture the variable interaction through the use of visualization. The framework for this study is the analytical hierarchy process (AHP) theory (**Figure 1**). **Figure 1** also presents the interaction between AHP theory, information assurance, and resource inputs and outcomes. AHP is a decision-aiding method developed by [4].

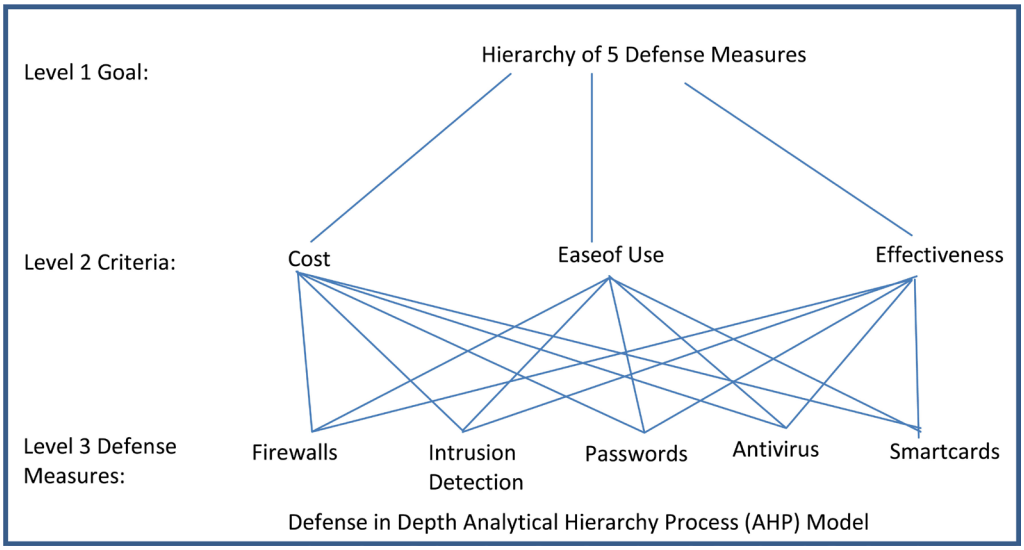

Figure 1. Hierarchy of five defense measures.

The study's theoretical/conceptual framework, shown in **Figure 1**, identifies how information assurance variables interact with cost, ease of use, and effectiveness variables.

According to an [5] article, "the goal is to quantify relative priorities for a given set of alternatives on a ratio scale, based on the judgment of the decision-maker, and stresses the importance of the intuitive judgments of a decision-maker, as well as the consistency of the comparison of alternatives in the decision-making process", using AHP methodology, a list of five information security elements was identified and their relative importance was evaluated for this research. Often, new models or theories are built by conducting scholarly research.

2. Results

The purpose of this chapter is to present the analysis which rejects the H_0 null hypothesis that AHP does not affect the relationship between the information technology analysts' prioritization of five defense in-depth dependent variables (anti-virus; firewalls; intrusion detection systems; passwords; and encryptions) and the independent variables of cost, ease of use, and effectiveness in protecting organizational devices against cyber-attacks. The data capture (recording) and coding methodology employed in this study was used to determine the best defense in-depth choices from a list of decision alternatives. Finally, a summary of the results are included in this chapter.

Investigative Questions

The study design included nine investigative questions which provided foundation for the main research questions. This section lists each investigative question and includes the statistical analysis to explore each sub question.

Investigative Question 1

Of the five most common information assurance measures (firewalls, intrusion

Table 1. Implementation cost pair-wise comparison.

Pair-wise Comparison	Implementation Cost				
	Passwords	Antivirus	Firewalls	Smartcards	IDS
A. Passwords (3.76)	1.00	1.21	1.25	1.42	1.51
B. Antivirus (3.10)	3.10	1.00	1.03	1.17	1.24
C. Firewalls (3.00)	3.00	0.97	1.00	1.13	1.20
D. Smartcards (2.65)	2.65	0.85	0.88	1.00	1.06
E. IDS (2.49)	2.49	0.80	0.83	0.94	1.00
Sum	12.24	4.84	5.00	5.66	6.02

Table 2. Implementation cost standardized matrix.

Standardized Matrix	Implementation Cost					
	Passwords	Antivirus	Firewalls	Smartcards	IDS	W-Vector (Weight)
A. Passwords (3.76)	0.31	0.25	0.25	0.25	0.25	26.20%
B. Antivirus (3.10)	0.25	0.21	0.21	0.21	0.21	21.60%
C. Firewalls (3.00)	0.25	0.20	0.20	0.20	0.20	20.90%
D. Smartcards 2.65)	0.22	0.18	0.18	0.18	0.18	18.46%
E. IDS (2.49)	0.20	0.17	0.17	0.17	0.17	17.35%
Sum	1.2254902	1	1	1	1	

detection systems, passwords, and smartcards); rank them in terms of cost of implementation with 1 being the least costly and 5 being the most costly. A pair-wise comparison is shown in Table 1, and a hierarchical synthesis used to weight the eigenvectors is shown in Table 2.

The consistency index (CI) $(\Lambda\max - n)/(n - 1)$, gives information about logical consistency among pair-wise comparison judgments in a perfect pair-wise comparison case. When CI = 0.0, there is no logical inconsistency among the pair-wise comparison judgments, or the judgment is considered 100% consistent [6]. The consistency ratio (CR) is a measure of how consistent the judgments have been relative to large samples of purely random judgements. If the CR is much in excess of 0.1, the judgments are untrustworthy [7].

In Table 3, the consistency ratio is provided. The consistency ratio of 0.01 shows that the pair-wise comparison does not exceed 0.10 and is considered acceptable. The results of the information technology analyst survey and the AHP consistency index table (Table 3) show that passwords have moderately (6.55) less implementation cost than the other four information assurance measures.

3. Discussion

The knowledge gained from this investigation can help in the prioritization of information assurance defense in-depth and in the evolution of the existing frameworks. The results show that passwords are moderately (6.26) easier for management to use in comparison to the other four information assurance

Table 3. Implementation cost consistency index.

Consistency Index	Implementation Cost						
	Passwords	Antivirus	Firewalls	Smartcards	IDS	Sum	W-Vector (Weight)
A. Passwords (3.76)	0.31	0.25	0.25	0.25	0.25	1.31	6.55
B. Antivirus (3.10)	0.25	0.21	0.21	0.21	0.21	1.08	5.40
C. Firewalls (3.00)	0.25	0.20	0.20	0.20	0.20	1.05	5.23
D. Smartcards (2.65)	0.22	0.18	0.18	0.18	0.18	0.92	4.62
E. IDS (2.49)	0.20	0.17	0.17	0.17	0.17	0.87	4.34
						Lambda	5.23
					Consistency Index	CI	0.05
					Consistency Ratio	CR	0.01

Note. $p = cr < 0.10$.

measures and can be used by managers who have less information assurance training. Passwords also have moderately (6.38) less maintenance cost than the other four information assurance measures and can be used by organizations that operate on a limited budget. Additionally, firewalls are slightly (5.70) easier for employees to use in comparison to the other four information assurance measures. This can make it easier for personnel intensive organizations to prioritize defense in-depth measures. The results show that firewalls are significantly (7.88) more effective at stopping DoS attacks in comparison to the other four information assurance measures can be used to lower the number of attacks that organizations face.

4. Conclusions

The research concluded that the AHP process can play a role in the IT security of organizations. Further research of the current use of defense in-depth and potential weaknesses of current information assurance procedures may help advance IT security overall.

The research conclusion that the AHP process can be used to prioritize defense in-depth measures is affirmed, given the significant amount of AHP knowledge that is published. The integration of the AHP process in defense in-depth decision-making can help to improve IT security. The use and implementation of AHP to prioritize defense in-depth measures could be an added asset in many organizations.

Future research into the AHP, especially related to IT security may help improve the understanding of how to design and deploy defense in-depth measures. This study also proposed an AHP structural and measurement model to help determine important factors in better understanding and implementing AHP in IT security solutions. The future of IT security should include additional exploratory models to advance understanding of why the current models are not substantially improving IT security.

5. Methodology

5.1. Research Design

This non-experimental survey research design was used to survey a simple random sample frame of 954 active Survey Monkey registered information technology analysts. A link to the survey was emailed to Survey Monkey registered information technology analysts, asking them to prioritize five defense in-depth measures based on standard cost, perceived ease of use, and effectiveness. The prioritization was done using a Likert scale instrument with a (1 - 5) prioritization of the five measures.

5.2. Data Analysis

The data analysis was conducted using a Likert Scale, with a (1 - 5) prioritization of the five defense in-depth measures and the AHP model to conduct a pair-wise comparison of each of the five measures. The research methods used in the study provided the advantage of using statistics to make inferences about larger groups, using very small samples, referred to as generalizability [8]. The findings are presented in the results section.

Acknowledgements

Capella University Dissertation Committee.

Declarations

Ethical Considerations

The potential benefits of research in organizations, especially public safety organizations, can be very beneficial, but there are risks that some employees or the organization could be unfairly stigmatized. This study was conducted with the informed consent of all of the participants. The participants were not subjected to risk. To avoid conflict of interest, the survey participants are in no way related to the researcher.

Consent for Publication

For specifically addressing autonomous agency, the design included an informed consent process to ensure that participation was voluntary, with adequate information provided to participants to make their decision of whether or not to participate [9]. Specifically addressing diminished autonomy, while ensuring extra protection is afforded to prevent harm from exclusion, and the design used a web-based online survey methodology with potential participants included from a compiled database of IT security professionals.

Availability of Data and Material

All datasets on which the conclusions of the manuscript rely will be deposited in publicly available repositories (where available and appropriate) supporting files, in machine-readable format (such as spreadsheets rather than PDFs).

Competing Interests

The author has no financial and non-financial competing interests.

Authors' Contributions

Rodney Alexander is the sole author of this article.

References

[1] Biesecker, C. (2010) DHS IG Finds Adequate Cyber Security Controls but More Needed. *Defense Daily*, **247**, 8.

[2] Lawrence, D.P. (2013) Impact Assessment: Practical Solutions to Recurrent Problems and Contemporary. 2nd Edition, Wiley & Sons, Hoboken. https://doi.org/10.1002/9781118678381

[3] Basagiannis, S., Petridou, S., Alexiou, N., Papadimitriou, G. and Katsaros, P. (2011) Quantitative Analysis of a Certified e-Mail Protocol in Mobile Environments: A Probabilistic Model Checking Approach. *Computers & Security*, **30**, 257-272. https://doi.org/10.1016/j.cose.2011.02.001

[4] Saaty, T.L. (1994) How to Make a Decision: The Analytic Hierarchy Process. *Interfaces*, **24**, 19-43. https://doi.org/10.1287/inte.24.6.19

[5] Al-Harbi, K. (2001) Application of the AHP in Project Management. *International Journal of Project Management*, **19**, 19-27.

[6] Utugizaki, M., Udagawa, M., Shinohara, M. and Osawa, K. (2007) Consistency Index for the Whole Decision Making. *Proceedings of DEA Symposium* 2007, Osaka University, Osaka, 102-105.

[7] Geoff, C. (2004) The Analytic Hierarchy Process (AHP). Pearson Education, Upper Saddle River.

[8] Cooper, C.R. and Schindler, P.S. (2008) Business Research Methods. 10th Edition, McGraw-Hill, Boston.

[9] National Commission for the Protection of Human Subjects (1979) Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research. Department of Health and Welfare, Washington DC.

[10] Rouse, M. (2007) Defense in Depth. http://searchsecurity.techtarget.com/definition/defense-in-depth

[11] Effectiveness. http://www.businessdictionary.com/definition/effectiveness.html

[12] Cobb, M. (2014) Firewall. http://searchsecurity.techtarget.com/definition/firewall

[13] Cole, B. (2014) Intrusion Detection System. http://searchcompliance.techtarget.com/definition/intrusion-detection-systems-IDS

[14] Alexander, M. (2012) Making Use of the Analytic Hierarchy Process (AHP) and SAS/IML. Social Security Administration, Baltimore, MD.

[15] Rouse, M. (2007) Password. http://searchsecurity.techtarget.com/definition/password

[16] Davis, F.D. (1989) Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, **13**, 319-340. https://doi.org/10.2307/249008

[17] Cobb, M. and Meckley, J. (2016) Smart Card. http://searchsecurity.techtarget.com/definition/smart-card

[18] Standard Cost (n.d.). In Business Dictionary. http://www.businessdictionary.com/definition/standard-cost.html

List of Abbreviations

Consistency index (CI). (Λmax − n)/(n − 1) gives information about logical consistency among pairwise comparison judgments in a perfect pairwise comparison case. When CI = 0.0, there is no logical inconsistency among the pairwise comparison judgments, or the judgment is considered 100% consistent [6].

Consistency Ratio (CR). A measure of how consistent the judgments have been, relative to large samples of purely random judgements. If the CR is in excess of 0.1, the judgements are untrustworthy [7].

Defense in-depth.

"Defense in-depth is the coordinated use of multiple security countermeasures to protect the integrity of the information assets in an enterprise. The strategy is based on the military principle that it is more difficult for an enemy to defeat a complex and multi-layered defense system than to penetrate a single barrier" [10].

Effectiveness. "The degrees to which objectives are achieved and the extent to which targeted problems are solved" [11].

Firewall. "A firewall is a network security system, either hardware- or software-based, that controls incoming and outgoing network traffic based on a set of rules" [12].

Intrusion detection system. Host intrusion detection systems and network intrusion detection systems are methods of security management for computers and networks [13].

Lambda. The value equal to the number of factors in the comparison (n=4) for total consistency [14].

Password. "A password is an un-spaced sequence of characters used to determine that a computer user requesting access to a computer system is really that particular user" [15].

Perceived ease of use. Perceived ease of use is the degree to which an individual believes that using a particular system would be free of physical and mental efforts [16].

Smart card. A smart card is a plastic card about the size of a credit card with an embedded microchip that can be loaded with data, used for telephone calling, electronic cash payments, and other applications, and then periodically refreshed for additional use [17].

Standard cost. "An estimated or predetermined cost of performing an operation or producing a good or service, under normal conditions" [18].

W-vector (Eigenvectors). Eigenvectors are derived from the eigenvalues of normalized measures, *i.e.*, the proportion of the row/column factors divided the row/column sum [14].