ITMSOC

Available online at http://itmsoc.org

Information Technology Management Society

ITMSOC Transactions on Innovation & Business Engineering 01 (2016) 34–39

ITMSOC–IBE
ITMSOC Transactions on Innovation and Business Engineering

http://www.itmsoc.org

Value Analysis of Cyber Security Based on Attack Types

Mehrnaz Akbari Roumani*, Chun Che Fung, Shri Rai, Hong Xie

School of Engineering and Information Technology, Murdoch University, Perth, Australia

Received 29 January 2016; Accepted 15 September 2016

Abstract

It is challenging to ensure security and to minimize economic impacts due to cyber-attacks because of the heavy reliance on ICT in different organizations and this paper presents an approach to estimate the cost of cyber security in public and private sector organizations. The paper also describes an approach for selecting the type of cyber security improvements to ensure that organizational goals are achieved. Different types of cyber-attacks and the subsequent impacts of these attacks are considered. A Value Analysis method is proposed to support the decision-making process by determining the priorities of deployment of various cyber security technologies. The proposed method is based on security costs related to and the losses due to attacks. Examples are provided in the paper to illustrate the proposed approach.

Keywords: Cyber-attack, Cyber Security, Value Analysis, IT Security Management.

1. Introduction

IT is recognized that cyber-attacks have different levels of negative impact to the performance of organizations with economic consequences. There are also different kinds of security technologies to address these issues. This forms the motivation of this study in proposing a value analysis method as a means or basis for determining the priorities of deployment of various security technologies.

Cyber security focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction. The important question is: How much an organization should invest in cyber security in order to minimize losses due to cyber-attacks? [2]. The situation is that both the investment in security measures and the loss sustained by the organization due to cyber-attacks are costs to the organization. In the real world, there is no definitive answer yet as to how these costs can be balanced or traded off.

A review of the literature shows that a number of approaches have been tried. In one approach, finding ROI (Return on Investment) is used [3, 4]. It has also been shown that ROI is a major consideration in the economics of information systems [5]. Using cost-benefit analysis and outcomes based on theoretical data, Loeb focused on Net Present Value (NPV) and Internal Rate of Return (IRR) [6]. Loeb's approach risk management and bypass rate for security technologies are used to assess investment in cybersecurity. Hahn and Govindarasu used attack tree and Petri nets with PENET software [7]. Bojanc defined a mathematical method using risk assessment of cyber-attacks [8, 9]. Interactions between attackers and organizations using game theory have also been considered [1, 10, 11]. While it is important to note that it is not possible to have 100 % security for organizations, it is still necessary to quantify the costs due to attacks, and investments needed to counter the problem.

This paper is organized as follows: Section 2 provides a discussion of different types of cyber-attacks and their associated costs. Section 3 discusses the available security technologies and

*Corresponding author.
Email address: M.akbariRoumani@murdoch.edu.au (Mehrnaz Akbari Roumani)

e-ISSN: 2539-5904

Table 1. Purchase and Installation of An Ids Hardware with Software to Support Audit Trials and Investigation [1].

Task	Cost		
	Small	**Medium**	**Large**
Purchase and Install Intrusion Detection System with Audit Trail Software	1 FTE, 1 day for installation; $750 per server IDS probe; plus $240 per workstation agent; plus $1,300 per manager/console, and/or $4,800 per network IDS probe; plus $2,400 for analysis console; 1 FTE, 3 months for monitoring IDS	1 FTE, 3 days; $750 per server IDS probe; plus $240 per workstation agent; plus $1,300 per manager/console, and/or $4,800 per network IDS probe; plus $2,400 for analysis console; 1 FTE, 6 months for monitoring IDS	1 FTE, 2 weeks; $750 per server IDS probe; plus $240 per workstation agent; plus $1,300 per manager/console, and/or $4,800 per network IDS probe; plus $2,400 for analysis console; 1 FTE, 1 year for monitoring IDS

their associated costs. Section 4 introduces the value analysis approach. Section 5 provides the value analysis method. Section 6 is an example for illustration purposes. Section 7 concludes this paper.

2. Types of Cyber-Attacks and Their Associated Losses

2.1. Types of Cyber-attacks

Undoubtedly, the goal of a secure information system for all organizations is challenging due to all forms of possible attacks. While many types of attacks have already been identified and defined [11], the most common types of attacks could be considered based on reports from the Ponemon Institute [12]. This forms an essential component in this study, given as:

- Viruses/Worms/Trojans,
- Malicious code,
- Phishing,
- Malware,
- Denial of service (DOS),
- Web-based attacks.

2.2. Losses due to Cyber-attacks

Losses due to these cyber-attacks could take many forms and different parts of an organization could be affected. In order to counter these attacks, it is vital for organizations and individuals to optimize the investment or expenses associated with cyber security, based on the various kinds of potential attacks. Studies from the Ponemon Institute have shown attacks have occurred in a wide spectrum of industry segments including utilities and energy, financial services, technology and education and research companies. The study in US shows that the utilities and energy industry suffered heavy losses of about 20 million dollars in both 2011 and 2012 [12]. Therefore, the study shows that attacks due to malicious code, DOS, Web based attacks and malicious insiders have amounted to over 60% of the total losses. Moreover, Virus/Worm/Trojan and malware are the most popular attacks with over 95% of the companies reporting experience of such attacks.

2.3. Effects of Security technology on Attacks

Security technologies are used to mitigate attacks. There are several reported studies on security technologies and their benefits [13]. Butler studied security technology benefit assessment and their effectiveness against each attack. For example, it was reported that network monitoring software reduced Distributed DOS (DDOS) by 75% [13]. Arora *et al*. proposed a framework to evaluate the cost/benefit of security measures by considering the effectiveness of security technology in preventing attacks based on bypass rates. The same study reported that firewalls have the ability to mitigate virus/worm by 20% [14]. These information are therefore used as basis of the analysis in this study.

3. Security Technologies and Their Costs

3.1. Cost Estimation for Security

One important and vital ingredient to protect an organization is the existence of a plan for cyber security and the associated budget. Based on National Institute of Standards and Technology (NIST), the cost estimates for IT security in an organization could be considered under a framework with three headings: management, operational and technical controls. These consist of 17 categories with further sub-divisions into guidance and tasks such as self-assessment, review, analysis, testing, contingency plan, etc. For each recommended process or tasks based on NIST standards, the budget can then be assessed. For example, the budget for the purchase and installation of an Intrusion Detection System (IDS) with Audit Trail Software based on the size of an organization is illustrated in Table 1. This meets the NIST standards 8.2.7, 11.2.4 - 11.2.5, 15.2.1, 16.1.1, 17.1.1 - 17.1.2, and 17.1.6 - 17.1.9 [15].

In Table 1, FTE is Full Time Employee and therefore, the cost of IT security measures for different organizations could be evaluated for the associated costs required to counter the attacks.

3.2. Security Technologies to Mitigate Cyber-Attacks

Security managers need to determine the security design and technologies to be used, and to estimate the effectiveness of each technologies against different kinds of attacks [10, 16]. There are four main security attributes: confidentiality, integrity, privacy and availability. It is important to understand the potential attack and the corresponding mitigation for each of the above attributes. Table 2 shows the possible attack methods and the technology needed to prevent such attacks [12].

Table 2. Attack Methods and Solutions [11].

Security Attributes	Attack Methods	Solution Technology
Confidentiality	Eavesdropping, Hacking, Phishing, DOS, and IP spoofing	IDS, Firewall, Cryptographic systems, IPSec, and SSL
Integrity	Viruses, Worms, Trojans, Eavesdropping, DOS, and IP spoofing	IDS, Firewall, Anti-Malware software, IPSec, and SSL
Privacy	Email Bombing, Spamming, Hacking, DOS, and cookies	IDS, Firewall, Anti-Malware Systems, IPSec and SSL
Availability	DOS, Email Bombing, Spamming, and System Boot Record Infectors	IDS, Firewall, and Anti-Malware software

Table 3 illustrates the NIST standards which consider the security technologies and their effects on each attack using a finer grain threat assessment [17].

4. Cyber Security and Value Analysis

4.1. Cost/Benefit in Information Technology

Based on previous studies, it is noted that security for organizations needs to be improved and the security approach used needs to be matched to the threat that exists using a cost-benefit model. Some studies have already been carried out to find such models. For instance, a framework to evaluate the costs and benefit of IT security was established by Arora *et al*. [14], based on observed damages, cost for existing security, and bypass rates. Furthermore, Xie *et al*. considered a hierarchical cost-benefit analysis to estimate the cost of establishing the information security improvement plans [13]. The question that remains is how much will be required to be spent on each part of the market/service layer in order to improve the security without blowing out the budget. The aim of cost-benefit analysis is for decision support to assist management and in budget planning [6]. In the next section, a value analysis to make targeted improvements to a system's cyber security is introduced. The approach is proposed as a tool to aid decision-making in value engineering.

Table 3. Typical Effectiveness (High, Medium, Low) against Attacks [17].

Technologies	Malware Type					
	Multipartite Virus	Macro Virus	Network Service Worm	Mass Mailing Worm	Trojan Horse	Malicious Code
Security Tools:						
Anti-virus	H	H	H	H	H	H
Anti-malware	H	H	H	H	H	H
Spyware detection and removal utility					H	H
Network-based intrusion detection system			L	L		
Host-based intrusion detection system			L		L	L
Network-based spam filtering				L-M	L	L
Host-based spam filtering				L-M	L	L
Network-based Web content filtering					L	L
Host-based Web content filtering					L	L
Network Configuration Changes:						
Network-based firewall			H	M		M
Host-based firewall			H			M
Internet border router			H			M
Internal router			H			M
Network Configuration Changes:						
Host hardening (including patching)	L	L	M	M	M	M
E-mail server setting	L	L		L-M	L	L
Setting for other services housed			L-M			
Application client setting		M	M			M

4.2. Value Analysis

One of the established models related to this proposed work is the Tanaka model of Value Analysis. In 1985, Tanaka [15] proposed a method to optimize a value that has a direct relationship to importance and an inverse relationship to cost. Value analysis is an approach to optimize an item's value by considering the importance and the cost of that item. This value could be for a system, a process, a procedure, a plan, a tool or a service. In value analysis, the value of the item is not the same as the item's cost. The approach is illustrated with the expression below:

$$VI = \frac{RP}{RC}, \tag{1}$$

where,

VI: the value of an item (i.e. $Value\ \ Index$);

RP: the relative performance (importance) of its function;

RC: the relative cost of the item.

An optimal value can be considered when the cost and importance of the value is the same, that is, $Value\ \ Index = 1$. A value index of more than one indicates improved performance of the item, and a value index less than one means that it is necessary to reduce the cost. However, Tanaka argued that this is too restrictive. Therefore, an optimal value zone was considered. Tanaka has shown that it could be possible to find an optimization limit, based on the importance and spending cost on the system components [18]. Tanaka's control limit was found as follows:

$$\begin{aligned} CLu &= \sqrt{x^2 + q^2}, \\ CLl &= \sqrt{x^2 - q^2}, \end{aligned} \tag{2}$$

where,

CLu: the optimal upper limit;

CLl: the optimal lower limit;

x: the percentage relative importance;

q: the percentage instance value (tolerance determined by management);

Values inside the optimal zone are considered to be the best value indices.

The challenge is to relate this value analysis to decisions concerning the security of the organization. This will be discussed in the next section.

5. A Value Analysis Method for Cyber Security

Cyber security depends on the requirements, policies, approaches and technologies. Therefore, the required cost of cyber security is also based on the same things. On the other hand, the cost of cyber-attacks is related to losses due to cyber-attacks. The proposed value analysis approach is therefore based on the estimated losses due to each attack, and the spending cost for the cyber security measures in order to counter each type of attack. The value indices could then be calculated from the following equation:

$$V = I/C, \tag{3}$$

where,

V: the value index of attack;

I: the importance index of attack;

C: the security Cost index for attack.

Using the Tanaka optimal zone, the control limit will be found using Eq. (2).

5.1. Importance Value Index

The Importance Value Index for the attack is based on the cost suffered when an attack occurs. This index is based on frequency of attack and the loss is calculated as:

$$L_i = \frac{L_i}{\sum_{i=1}^{k} L_i}, \tag{4}$$

where, L_i: the losses due to attack, i, in a particular period.

5.2. Security Cost Index for Attack

This index represents the cost of the protective security measures to guard against attacks, and it could be found as follows:

$$C_i = \frac{\sum_{j=1}^{m} \rho_{ij} \times SC_j}{\sum_{i=1}^{k}\sum_{j=1}^{m} \rho_{ij} \times SC_j}, \tag{5}$$

and

$$\rho_i = \frac{\rho_{ij}^o}{\sum_{j=1}^{m} \rho_{ij}^o}, \tag{6}$$

where,

C_i: the value of security cost index for attack i;

SC_j: the cost of security technology j;

ρ_{ij}: the normalized coefficient for security technology j based on attack i;

ρ_{ij}^o: the initial coefficient for security technology j based on attack i.

These values could be estimated based on standards, data from other studies and the determination could be made by security experts [1, 12, 16]. The following section uses an example to illustrate the proposed approach.

6. An Example To Illustrate The Value Analysis Approach

Using actual data from the Ponemon report [12], the importance index on losses due to each cyber-attack can be derived using Eq. (4). Hence, with Eqs. (5) and (6), the cost of cyber security for each attack is calculated. Using these results, the value index for each attack could be found from Eq. (3). Table 4 shows these indices for five types of cyber-attacks on medium sized companies in the US.

These cyber security value indices for all the attacks and the control limit have been shown in Fig. 1 by considering $q = 0.2$. With respect to the value analysis results from US companies, the following observations are made:

Table 4. Cyber Security Value Index for US companies.

Index	Type of attacks				
	Virus/Worm/Trojan	Malware	Malicious code	Phishing	DOS/DDOS
Importance (%)	11	6	41	11	31
Cost (%)	13	17	30	33	7
Value	0.85	0.35	1.37	0.33	4.43

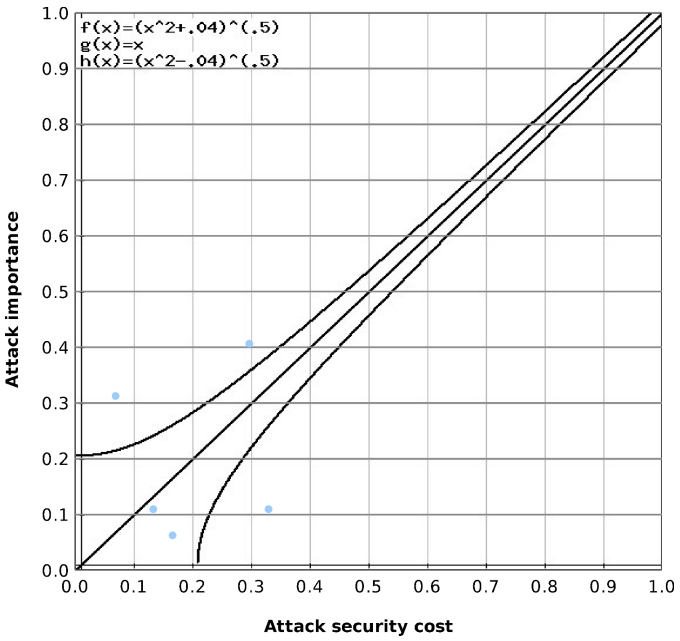

Fig. 1. Cyber security control limit and value graph for US companies.

- Value index for DOS and malicious code are above optimal zone, hence, these companies need to review their security policies and technologies in order to improve their protection against such attacks. Additional expenses may also be required in these areas.
- For virus/worm/trojan and malware attacks, the value analysis results indicated that they are in the optimal zone. This means the existing expenditures on cyber security for these areas are sufficient.
- Phishing attack is under optimal zone and the companies need to review their security policies and technologies. They may be able to maintain the existing practices while reducing the budget for this type of attacks saving costs for the company.

7. Conclusions

Finding the priorities for the investment or expenses to ensure cyber security is an important issue for an organization's planning and budget. This paper proposes the use of a Value Analysis approach as a means to find the priorities in dealing with cyber security. An example using the proposed approach to manage cyber-attacks is provided and the results are used for illustration purposes. The next phase of the study will focus on the expansion of the model and collection of larger and practical data set to verify the model and the approach.

References

1. Department of Education. Information Technology Security Cost Estimation. Department of Education; 2002. Available from: https://www.hitpages.com/doc/6465573437308928/1.
2. Roumani MA, Fung CC, Choejey P. Assessing economic impact due to cyber attacks with System Dynamics approach. In: 2015 12th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON). Institute of Electrical & Electronics Engineers (IEEE); 2015. Available from: http://dx.doi.org/10.1109/ECTICon.2015.7207084.
3. Li H, Gong S, Lai L, Han Z, Qiu RC, Yang D. Efficient and Secure Wireless Communications for Advanced Metering Infrastructure in Smart Grids. IEEE Transactions on Smart Grid. 2012 Sep;3(3):1540–1551. Available from: http://dx.doi.org/10.1109/TSG.2012.2203156.
4. Longstaff TA, Chittister C, Pethia R, Haimes YY. Are we forgetting the risks of information technology? Computer. 2000 Dec;33(12):43–51. Available from: http://dx.doi.org/10.1109/2.889092.
5. Yan Y, Qian Y, Sharif H. A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid. In: 2011 IEEE Wireless Communications and Networking Conference. Institute of Electrical & Electronics Engineers (IEEE); 2011. Available from: http://dx.doi.org/10.1109/WCNC.2011.5779257.
6. Gordon L, Loeb M. Managing Cybersecurity Resources: A Cost-Benefit Analysis (The Mcgraw-Hill Homeland Security Series). McGraw-Hill Education; 2005. Available from: http://www.amazon.com/Managing-Cybersecurity-Resources-Cost-Benefit-Mcgraw-Hill/dp/0071452850%3FSubscriptionId%3D0JYN1NVW651KCA56C102%26tag%3Dtechkie-20%26linkCode%3Dxm2%26camp%3D2025%26creative%3D165953%26creativeASIN%3D0071452850.
7. Hahn A, Govindarasu M. Cyber Attack Exposure Evaluation Framework for the Smart Grid. IEEE Transactions on Smart Grid. 2011 Dec;2(4):835–843. Available from: http://dx.doi.org/10.1109/TSG.2011.2163829.
8. Bojanc R. In: Quantitative Model for Information Security Risk Management. Knowledge and Learning: Global Empowerment; Proceedings of the Management, Knowledge and Learning International Conference 2012. International School for Social and Business Studies, Celje, Slovenia; 2012. p. 267–275. Available from: https://ideas.repec.org/h/isv/mklp12/267-275.html.
9. Bojanc R, Jerman-BlaÅi B. An economic modelling approach to information security risk management. International Journal of Information Management. 2008 Oct;28(5):413–422. Available from: http://dx.doi.org/10.1016/j.ijinfomgt.2008.02.002.
10. Butler SA. Security attribute evaluation method. In: Proceedings of the 24th international conference on Software engineering - ICSE 02. Association for

Computing Machinery (ACM); 2002. Available from: http://dx.doi.org/10.1145/581339.581370.
11. Adeyinka O. Internet Attack Methods and Internet Security Technology. In: 2008 Second Asia International Conference on Modelling & Simulation (AMS). Institute of Electrical & Electronics Engineers (IEEE); 2008. Available from: http://dx.doi.org/10.1109/AMS.2008.68.
12. Ponemon Institute. 2012 Cost of Cyber Crime Study: United State. Ponemon Institute; 2012. Available from: http://static.knowledgevision.com/account/idgenterprise/assets/attachment/HPESP_WP_PonemonCostofCyberCrimeStudy2012_US.pdf.
13. Xie N, Mead N, Chen P, Dean M, Lopez L, Ojoko-Adams D, et al. SQUARE Project: Cost/Benefit Analysis Framework for Information Security Improvement Projects in Small Companies. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University; 2004. CMU/SEI-2004-TN-045. Available from: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=7013.
14. Arora A, Hall D, Piato CA, Ramsey D, Telang R. Measuring the risk-based value of IT security solutions. IT Prof. 2004 Nov;6(6):35–42. Available from: http://dx.doi.org/10.1109/MITP.2004.89.
15. TANAKA M. New approach to the function evaluation system in value engineering. International Journal of Production Research. 1985 Jan;23(4):625–637. Available from: http://dx.doi.org/10.1080/00207548508904733.
16. Cleveland FM. Cyber security issues for Advanced Metering Infrasttructure (AMI). In: 2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century. Institute of Electrical & Electronics Engineers (IEEE); 2008. Available from: http://dx.doi.org/10.1109/PES.2008.4596535.
17. Mell P, Kent K, Nusbaum J. 2012 Cost of Cyber Crime Study: United State. National Institute of Standards and Technology (NIST); 2012. Available from: http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf.
18. Yoshikawa T, Innes J, Tanak M, Mitchell F. Contemporary Cost Management. Chapman & Hall; 1993. Available from: http://www.amazon.com/Contemporary-Cost-Management-Takeo-Yoshikawa/dp/0412452103%3FSubscriptionId%3D0JYN1NVW651KCA56C102%26tag%3Dtechkie-20%26linkCode%3Dxm2%26camp%3D2025%26creative%3D165953%26creativeASIN%3D0412452103.