Information asset modelling for risk analysis

Y. G. Sung, P. Kang & W. T. Sim
Cylab Korea, Korea Information Security Agency, Republic of Korea

Abstract

An information technology-driven organization, in which most business is carried out and its revenue is presented through information technology, increasingly provides their key functions through computer systems and networks. These kinds of environments have prompted every day cyber threats through computer technology and Internet infrastructure. Current issues are rising for the matter of risk analysis on information technology transactions. To fulfil accurate risk estimation of this, different approaches are required to consider what each information asset is and what cyber vulnerabilities it is open to. In order to succeed, first it is necessary to identify its model of information asset, unlike conventional assets where each asset can be figured out as a whole value, then measure the value of it. In this paper, we are trying to show the methods and approaches to applying risk analysis to the information technology field. Hereafter, we identify key elements consisting of assets of a computer system. After its completion, we create a mathematic function to calculate its value based on the asset elements. The research results will yield an implementation of an automatic risk assessment tool for computer networks.
Keywords: information asset, risk analysis, computer network, security vulnerability, impact value.

1 Introduction

Many companies are increasingly relying on computer systems for their business, where large amounts of network traffic rise every day to operate its business and individual staff work on personal computers. To predict and minimize the risk of network attack, traffic analysis measurement techniques should be in place after monitoring tools are deployed: when inbound and outbound traffic is out of normal levels, the network administrator can make the

WIT Transactions on The Built Environment, Vol 94, © 2007 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE070051

decision that the computer network might have unidentified attacks. However, to precisely foresee potential risks for the critical assets, further variables in it like service or software information should be considered.

In terms of asset-oriented risk assessment, corporate management just has interests in their IT asset for the perspective of whether it is safe or not since corporate value is created and fulfilled through services or data residing in IT assets. Therefore the purpose of this paper is, regarding IT asset-oriented risk assessment, to show how to set asset values and weighting using traffic amounts. Network managers or operators can realize this on the use of network monitoring implementations.

This paper is described as follows. Section 2 gives the background of making the information asset model. Section 3 states the components of an information asset, in section 4 there is a suggested function to calculate the value of an information asset to predict the impact of loss of an asset. In sections 5 and 6, future research is pointed out and conclusive remarks made.

2 Background

The risk analysis process, suggested in NIST 800-30 [1] and OCTAVE^{SM} [2], gives the following six standard steps from asset identification to risk level determination. The following is a short description of risk determination.

1st Step. Asset Identification: In order to analyze a target information system, as the first step, core information assets are investigated.

2nd Step. Threat Analysis: Threat analysis addresses threat agent, motivation, and activity with any vulnerability.

3rd Step. Vulnerability Analysis: This is to find any weakness of the identified information asset for the threat agent to exploit.

4th Step. Attack Likelihood Determination: This is to calculate the likelihood of attack with agent motivation, vulnerability nature and current control implemented in the information system.

5th Step. Impact Analysis: This is to measure the negative effect if any attack is successful to vulnerability.

6th Step. Risk Level Determination: The risk of each asset is calculated and then the assets are prioritized in order.

Surveyed in the field of information system operators in Korea, a hardware system is considered to be a component of an information asset, and then a simple CIA (confidentiality, integrity and availability) pointing method is usually applied to prioritize the value of each asset. That is, they just give 3 level points (3, 2 and 1) to each CIA factor then summarize them; points can vary

from a minimum 0 to a maximum 9. Later this value is adjusted to the extent that the organization has a reasonable asset weight, where it ranges from 0 to 1. Most of these calculations, however, are determined by analysts' or system operator's intuition. There are no objective criteria and it is almost impossible to implement the process automatically without human intervention.

To achieve systematic and automatic assessment of Internet-relying corporate risk levels for computer systems in this paper, we judge that it is most important to set asset scope and boundary in the context of automatic measurement, and then expect the cost of impact for loss of the corporate information asset. Here with issues, we deal with researches on asset scoping, and its value determination for impact expectation. These asset value modelling approaches are in the process of implementing automatic risk assessment throughout the steps stated before. We also will address the way of how to automatically assess the impact value of an asset.

3 Information asset components

3.1 Issue and approach

Information assets, as through a computer network, are becoming a fundamental corporate sales raising factor to perform organisational activities, where entrepreneurs actively applies IT to the sales like an internet shopping mall, internet portal service firms, on-line banking system and telecommunication carrier.

In the risk analysis approach, the first step is how to figure out their asset scope. Even for computer system, the information asset to be protected might be its hardware, software, electronic data, process or functions. The view can be very varied. But the way of identifying the asset is its system's view [3], where we know everything in it. Otherwise, most risk analysts and consultants inter-mix methods by network analysis and system analysis when they need to get vulnerabilities into it. This way might collect unnecessary information or make it impossible to have numeric result.

Unlike prevalent methods realized in the field, we here see information assets as network and remote hacker perspective because risk assessment also focuses on predicting intrusion from the network path; for IT-driven and computer network-dependent companies, the asset to protect is primarily computer system resource to continue their business, and the primary issue is live networking and protection from any attacks or incidents.

3.2 What consists of information asset from network view

Internet businesses which make most their revenue through computers and internet media largely depend on computer security and safety, or the volume of bandwidth. For an internet shopping mall that busily runs hundreds or thousands of web servers in a DMZ area like figure 1, and then a confidential database server is put behind a firewall system. Web servers consume most of their access traffic from outside.

To assess the risk of a server, the first step is to know how much value a server is to predict an adverse effect for unavailability. Since the main resource to make revenue is the computer, we try to appraise the value of the computer system.

As found out by the field survey, most companies run their information systems like figure 1, where a corporate computer network is shown which makes profit using the web and databases computer hosts; databases server opens SQL service by port 443, and web server's service is open to the public through port 80. Outside users come in first to a web server, and then it connects to the database server if the user request has any relation with the database server, and then web server gives the results to the user. If any web severs or database stops, corporate business stops.

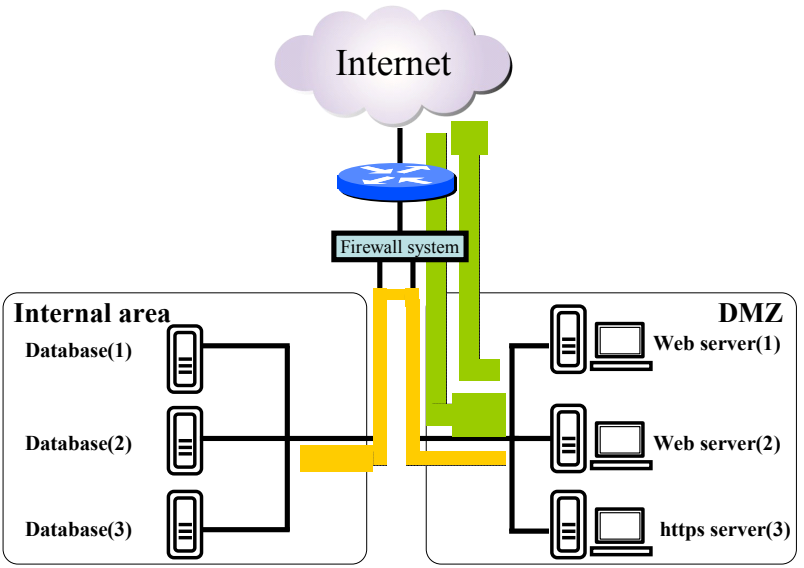

Figure 1: Typical network comprising Web and Database servers.

For the matter raised, we try to distract factors from the computer network perspective which will result in the way of anticipating quantitative value. In the context of this view and the nature of computer networks, those are computer IP addresses, network service, software regarding service and traffic dominant rate (tdr), and the number of visitors. From the network perspective, information asset consisting of parts may be internet protocol (IP), operating system, open port (service) and software information. After identifying the information asset through passive packet monitoring and active information gathering using *nmap*-like tool, all of the assets map can found from individual computer c_i to a set of computer assets C ($c_i \in C$). Hereafter computer asset (c_i) can be described as follows:

$$c_i = (ip_i, sv_{ik}, sw_{ik}, tdr_i, x_{ik}) \tag{1}$$

where *ip* is the unique asset identifier, *sv* is the service open to outside, *sw* is the running software on it, *tdr* is the network traffic dominant rate on each computer system in a segmented corporate network, and *x* is the number of site visitors. These factors are only relate to service availability issues; that is when computers are unavailable for service for the reasons like DoS attack, physical network device problem or administrative errors, company's sales amount can be directly affected.

As the volume of IT infra, even for IT company grows very large, the main concern is focusing on service connectivity. In the case of a big portal, it says that thousands of servers are running for service, so the potential of unavailability as well as security incidents of traditional confidentiality and integrity expands beyond one's imagination.

4 Measuring information asset value

4.1 Motive

Since the WWW service has opened and business based on the Internet has started, the opportunities for customers to use shopping malls and on-line bank services rise dramatically. Therefore, we guess that the number of site visits can be a key factor to promote corporate sales figure, so they depend highly on the volume of Internet traffic. We find out that sales volume is almost directly proportionate to Internet traffic (x), that is, the following equation can be anticipated.

$$| c_i | \propto x_i \tag{2}$$

By using the above simple assumption, we try to analyze each of the computer system's value ($|c_i|$) for 2 industry cases.

4.2 What is important factor among CIA

For the automatic and objective measurement of information assets, we try to analyze the relevance between the figure of traffic volume and its value for each internet-based industry. On-line sales grow in Internet banking, on-line shopping malls, and portal companies where Internet businesses prosper and grow as Internet users and traffic go up. They strategically monitor traffic movement to expect sales volume.

For the reasonable computation of asset value, we need to consider how big each portion of CIA is; is it that big for the impact for a breach of confidentiality and integrity issues, which is traditionally regarded as very critical? How much

wider is the corporate impact when its critical information, like electronic customer private data or price information stored in a database server is stolen or tampered with?

Table 1: Financial impact from confidential information disclosure incidents in bank in Korea.

		Y2003	Y2004	Y2005
Internet banking	Number of incidents	0	1	2
	Affected amount (K$)	0	3	68
Telephone banking	Number of incidents	1	5	6
	Affected amount (K$)	100	162	262
Total	Total number	1	6	8
	Total amount affected (K$)	**100**	**1,650**	**3,300**

[Source: The Bank of Korea, *http://www.bok.or.kr*].

As seen from a report from the Korea Central Bank in 2005, there have been bank account number disclosure incidents in recent years as seen from table 1. Even though most incidents are from the case that the bank account, bank access ID and password are stolen, the amount of financial damage from the incidents can be regarded as very small. For the year 2005, the total amount reached $3,300K.

In addition, there has been an incident reported in Korea that a man compromised price information in Internet shopping malls. He implemented a hacking module to tamper with the mall's goods' prices into 1% from the original price, then he visited 80 shopping sites and bought items at 1% of the true price. However the total affected amount only reaches about $12,000.

Unlike the above cases, the biggest Korean portal company had experience where it could not give a portal service for 3 hours 30 minutes in March 2006, and for 5 hours in July 2006. From these incidents the company finally cancelled its IT long-term outsourcing contract. This accident turned out to be a matter of a domain name mapping error and network device problem respectively, so the company received compensation for service unavailability.

The cases show that the financial damage from breach of confidentiality or integrity is relatively smaller than that of availability, and also the risk for service unavailability goes higher because of current complex and the giant configuration of computer networks.

These incident reports yield our decision that we can focus on just service unavailability cost for judging impact value of an asset. A decade ago, information disclosure was the main issue, so that the risk analysis for information disclosure has been tried [4]. Current security issues that move into unavailability risk out of traditional information disclosure or information tampering risk. The main risk in running IT systems from the service provider's perspective is addressed by availability outage. Consequently, in the process of valuing an asset, we can consider the service availability factor without including the impact of confidentiality and integrity damage. When necessary, weight can be imposed on the unavailability impact model.

4.3 Impact analysis

We made a hypothesis that for each industry field there are strong relationship between the increasing trend of Internet traffic and increasing pattern of sales volume. It is known that Internet traffic is doubling every six months, in other words, growing by 4 times annually [5], and accordingly internet business volume also expands.

Figure 2 shows a growing trend in the number of site visitors, at the same time the total on-line shopping mall's sales jumps 2 times.

4.3.1 Shopping mall case

To compare the correlation between traffic and sale value for an online shopping mall, we get 7-year data for a shopping mall with site visits and sales figure as shown in table 2 and figure 3.

The rest of the job is to find if there is some relevance between 2 variables. A plot is made using table 2 as seen in figure 3.

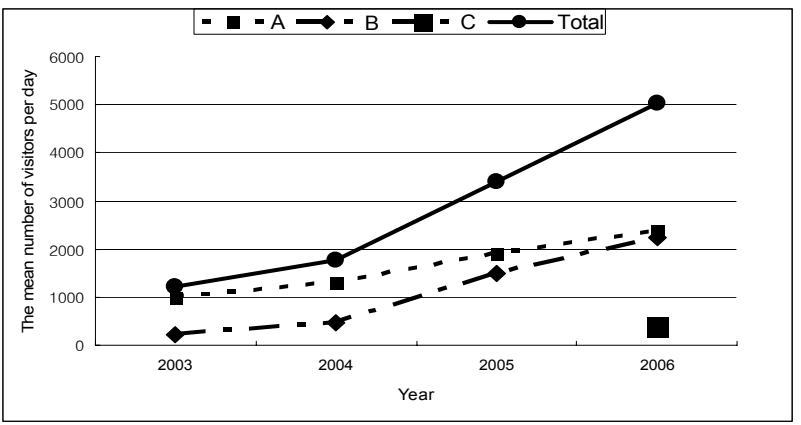

Figure 2: The yearly increasing number of visitors for 3 major shopping malls in Korea for 4 years. [Source: *http://www.rankey.com.*]

Table 2: The number of shopping mall visitors and sales amount per day.

Year	Mean site visitors per day	Mean site sales amount per day (thousand$)
2000	200,000	501.3
2001	400,000	824.9
2002	700,000	1393.9
2003	1,000,000	2465.7
2004	1,300,000	3205.4
2005	1,900,000	4657.5
2006	2,380,000	6849.3

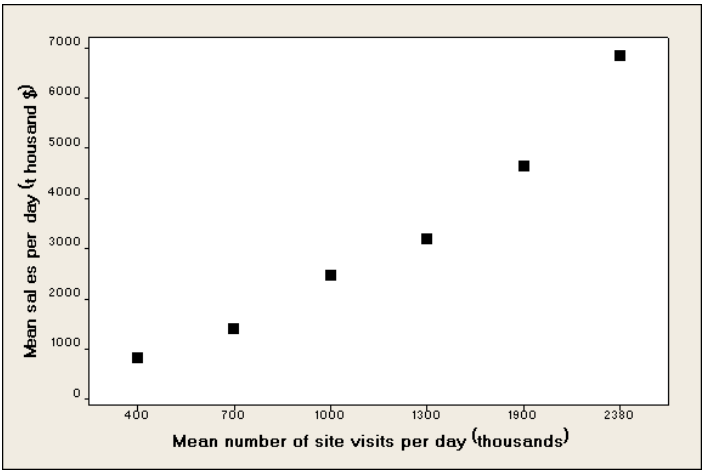

Figure 3: Daily visitor and sales relation plot for a shopping mall.

As assumed, because sales are dependent on the number of site visitor we put x as the daily visitors' number (unit is 1,000) as an independent variable, and y as the corresponding sales figure as a dependent variable (unit is $1,000). From regression analysis, coefficient and intercept is determined and its t-statistic value is 4.42, and P-value is 0.00685. We can get the following formula that has a correlation between daily site visiting numbers and sales amount.

$$y = 898.214 + 0.00108x^2 \tag{3}$$

Since equation (3) is expected sales figure per day, and we need to know that individual computer system value in the context of visit numbers, the formula can fit into following by multiplying individual system's traffic rate tdr_i;

$$y_{c_i} = (898.2 + 0.00108x^2)tdr_{c_i} \tag{4}$$

Equation (4) indicates we can figure out the loss impact ($|c_i|$) from result y_{ci} if a computer c_i is not available for any reason.

4.3.2 Portal site case

With similar methods, to analyze the portal's sales trend, we have obtained 5 year data of the number of site visitors and the yearly sales amount. Then its yearly data are divided into the daily number, which is shown in figure 4.

As assumed, because sales are dependent on the number of site visitor we put x as the daily visitor's number (unit is 1,000) as the independent variable, and y corresponding to the sales figure as the dependent variable (unit is $1,000). From regression analysis, coefficient and intercept is determined and its t-statistic value is -3.09, and P-value is 0.0363. We can get the following formula that has a correlation between daily site visiting numbers and the sales amount.

$$y = -592231 + 2x^2 \tag{5}$$

This figure show the corporate-wide total sales amount regarding the number of site visits per day. Therefore since we want to know that individual computer system value in the context of visit numbers, the formula can fit into the following (6) equation by multiplying individual system's traffic rate tdr_i;

$$y_{c_i} = (-592231 + 2x^2)tdr_{c_i} \tag{6}$$

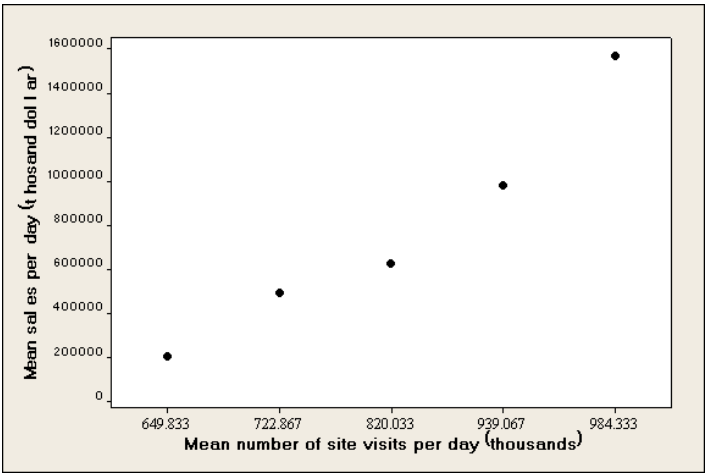

Figure 4: Daily visiting and sales relations plot for a portal.

5 Future task

There are many fields depending on computer networks which need risk analysis. We judge that for each field it has a different pattern or relationship between the number of site visitors and sales. Future task might have to focus on developing industry-specific models. The rest of this subject might concern Internet banking, travel agency, and even public service sites.

We do not consider the value of the asset itself; the purchasing and maintenance cost of each computer system because we guess that these kind of values can be negligible compared to the amount of calculated impact value. However, if operating cost can be measured automatically, it can be merged into the impact value.

6 Conclusion

As Internet infra is advanced and the usage price is going down, business on the Internet is incrementing every year. In an industry like a shopping mall, on-line sales have already surpassed off-line mall's sales. This phenomenon will get

much deeper. At the same time, the potential risk in IT areas are growing because complex networks are getting bigger, and the risk of damage by an intruder is growing. The risk management for computer networks and information systems are not optional, but a must today.

Therefore, in this paper, we show in the process of risk analysis, the network view of information assets and its valuation model from the asset factor for a shopping mall and portal service. This is the very first step for risk assessment to automate the risk assessment process. Our approach is a result of how to produce objective numeric values for a target computer system without analyst determination. By using this model, corporate CTO or IT managers can automatically control their computer system assets and its value. Further, its result can be applied to the risk assessment process to calculate the risk level.

References

[1] NIST SP 800-30, Risk Management Guide for Information Technology Systems.

[2] Christopher J. Alberts, Audrey J. Dorofee, OCTAVESM Criteria 2.0, CMU/SEI-2001-TR-016, December 2001.

[3] Yoon Jung Chung, Injung Kim, NamHoon Lee, Taek Lee, and Hoh Peter In, Security Risk Vector for Quantitative Asset Assessment, ICCSA 2005.

[4] Bodeaum, D.J., A Conceptual Model for Computer Security Risk Analysis, *Computer Security Applications Conference*, December 1992.

[5] Long-Term Traffic Statistics, http://www.cs.columbia.edu/~hgs/internet/.