

Evaluation of Information Security Investment Portfolios: A Probabilistic Approach

Tae-Sung Kim

kimts@chungbuk.ac.kr

Department of Management Information Systems, Chungbuk National University, Korea

Chandrasekhar Subramaniam

Sungjune Park

Ram Kumar

csubrama@uncc.edu

supark@uncc.edu

rlkumar@uncc.edu

Department of Business Information Systems and Operations Management

The University of North Carolina at Charlotte, USA

Abstract

As the impact of the information breaches to the information systems increases, organizations have a tendency not only to increase the information security budget but also to be sensitive to the information security expense. Organizations are faced with different types of security threats and they have several alternative technologies to mitigate the negative effects of the security threats. Most organizations implement a portfolio of the information security technologies. In this paper we suggest performance measures to evaluate information security systems, and evaluate information security investment portfolios.

1. Introduction

As the side effects of information society, for example, virus, unauthorized access, theft of proprietary information, denial of access, etc., diffuse, the information security becomes one of the most important issues for organizations. According to a survey by CSI/FBI, total losses resulted by security attacks or misuse amount to about \$130 million, and virus attacks alone resulted in about \$43 million to 700 organizations in 2005 (CSI 2005). In response to these security threats, organizations have implemented several security counter-measures such as firewalls, anti-virus software, intrusion detection systems (IDS), encryption (of data in transit and of files), smart cards, etc. A major growing concern for organizations is to evaluate and compare the performance of portfolios consisting of security counter-measures.

Recently many researchers have studied on economic aspects of information systems security. The first group of the literature is on assessment of the economic benefits of information

security investments. Gordon and Loeb (2002) provide an economic modeling framework for assessing the optimal amount to invest in information security to protect a given set of information. The second group is on the value of individual security technologies. Cavusoglu et al. (2005) assess the value of IDS in a firm's information technology security architecture. The third group is on guidelines for information security investment decision making. Cavusoglu et al. (2004) present an analytic model in an attempt to facilitate decisions regarding security investments. Bodin et al. (2005) show how a chief information security officer can apply the analytic hierarchy process (AHP) to determine the best way to spend a limited information security budget.

Most organizations implement a portfolio of the information security technologies and there is relatively little research on performance measures of information security systems consisting of multiple information security technologies. In this paper, we seek to offer performance measures of information security systems, and to evaluate information security investment portfolios.

This paper is organized as follows: Section 2 describes the probabilistic model of information security systems. Section 3 analyzes the model and derives the sojourn time of threats in the information security system. Section 4 presents a numerical example. Section 5 concludes the paper and suggests the future research topics.

2. Probabilistic Model of Information Security Systems

Assume that the information security systems to protect the information systems (infrastructure) of an organization consist of I types of information security technologies (counter-measures). Counter-measures are serially linked each other inside the information security system. J types of information threats arrive at the information system according to Poisson processes. If we assume that the information system manager installs the information security system ahead of the information system of the organization, threat j arrive at counter-measure i according to the Poisson process with rate λ_{ij} . Threat j arrived at counter-measure i receives a security service by counter-measure i and the service time is exponentially distributed with rate μ_{ij} . After receiving the service, threat j will be terminated if counter-measure i is effective on threat j with probability p_{ij} or threat j will be transferred to the next counter-measure with probability $1 - p_{ij}$. If all the counter-measures are ineffective on threat j , threat j arrives at the information infrastructure and definitely causes damages. When the damage

happens, recovery systems will be activated to recover the information system. Figure 1 describes the information security system having 3 counter-measures.

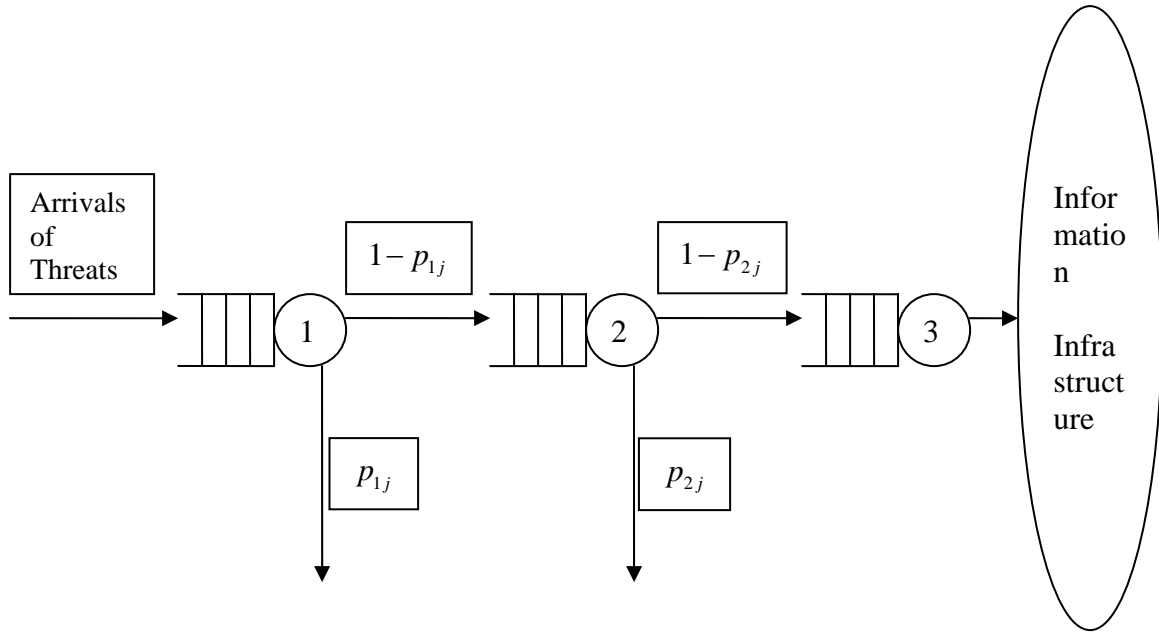


Figure 1. Information security system having 3 countermeasures

The notations in this paper are listed as follows:

- λ_{ij} : the arrival rate of threat j to counter-measure (service node) i (unit: number of threats per unit time);
- μ_{ij} : the service rate of counter-measure i for threat j (unit: number of threats per unit time);
- W_{ij} : the expected sojourn time of threat j in counter-measure i ;
- W_j : the expected sojourn time of threat j in the whole information security system;
- W : the expected sojourn time of an arbitrary threat in the whole information security system;
- m_i : the number of systems (units or capacity) or kinds in counter-measure i (i.e., number of servers at node i);
- p_{ij} : the effectiveness of counter-measure i on threat j ;
- $P_i(m_i)$: the probability of having m_i or more threats in counter-measure i ;
- α_{i0} : the probability of the queue in counter-measure i being empty.

In Figure 1, counter-measures 1 to 3 (node 1 to 3) can be preventive or detective information security technologies, and recovery system (node 4) is installed within the information infrastructure. Node 4 is the organization's information infrastructure and the threats passed by node 3 definitely cause damages, and W_{4j} (or $W_{(I+1)j}$ if there are I counter-measures) is the expected recovery time from the damage caused by threat j .

3. Sojourn Time of Threats in the Information Security System

If we consider 3 counter-measures and J types of threats, i.e., $i=1,2,3,4$; $j=1,\dots,J$, the expected sojourn time of threat j in the whole information security system can be obtained as

$$W_j = W_{1j} + (1 - p_{1j})W_{2j} + (1 - p_{1j})(1 - p_{2j})W_{3j} + (1 - p_{1j})(1 - p_{2j})(1 - p_{3j})W_{4j}. \quad (1)$$

W_{1j} is the sum of the waiting time of threat j in the queue until any server in node 1 begins to serve, and the expected service time of threat j in node 1. Threat j waits the expected service time of the server which ends first among m_1 servers only if the number of threats exceeds the number of servers in node 1. If all the servers in node 1 are still busy when the server which ends first completes its service, threat j waits additionally the expected service time of the server which ends first among m_1 servers. This process will continue until threat j is served.

If we let the service time of threat j in node i be X_{ij} , the probability that the threat of type k completes its service first among all the busy services is $\frac{\mu_{1k}}{\sum_{j=1}^J \mu_{1j}}$ (see Appendix A).

Because the service time of threat j at node 1 is exponentially distributed with rate μ_{1j} , the expected service time of threat j is $1/\mu_{1j}$. The expected service time of the server which ends first among m_1 servers can be obtained as follows:

$$\begin{aligned} & \sum_{k=1}^J \left[\{ \text{Pr}(\text{threat } k \text{ completes its service first among all the servers}) \} \right. \\ & \quad \left. \times \{ \text{expected service time of threat } k \} \right] \\ &= \sum_{k=1}^J \frac{\mu_{1k}}{\sum_{j=1}^J \mu_{1j}} \cdot \frac{1}{\mu_{1k}} = \frac{J}{\sum_{j=1}^J \mu_{1j}}. \end{aligned}$$

According to Kleinrock (1976), the probability that the number of threats exceeds the number of servers in node 1, that is, the probability of having m_1 or more threats in node 1,

$P_1(m_1)$, is $\frac{\alpha_{10} \cdot (m_1 \rho_1)^{m_1}}{m_1! (1-\rho_1)}$. And α_{10} , the probability of the queue of node 1 being empty, is

$\left[\sum_{k=0}^{m_1-1} \frac{(m_1 \rho_1)^k}{k!} + \frac{(m_1 \rho_1)^{m_1}}{m_1!} \cdot \frac{1}{1-\rho_1} \right]^{-1}$. Finally, the probability that all the servers in node 1 are

busy is $\rho_1 = \sum_{j=1}^J \frac{\lambda_{1j}}{m_1 \mu_{1j}}$. Then

$$\begin{aligned} W_{1j} &= \frac{1}{\mu_{1j}} + P_1(m_1) \left[\frac{J}{\sum_{j=1}^J \mu_{1j}} + \rho_1 \cdot \frac{J}{\sum_{j=1}^J \mu_{1j}} + \rho_1^2 \cdot \frac{J}{\sum_{j=1}^J \mu_{1j}} + \dots \right] \\ &= \frac{1}{\mu_{1j}} + P_1(m_1) \cdot \frac{J}{\sum_{j=1}^J \mu_{1j}} \cdot \frac{1}{1-\rho_1}. \end{aligned} \quad (2)$$

W_{2j} , W_{3j} and W_{4j} can be found likewise. From Equation (1), we can get W_j , the expected sojourn time of threat j in the whole information security system. And the expected sojourn time for an arbitrary threat in the information security system can be found as follows:

$$W = \sum_{j=1}^J \left(\frac{\lambda_{1j}}{\sum_{j=1}^J \lambda_{1j}} \right) W_j. \quad (3)$$

We can generalize the above results to the information security system having I counter-measures as follows:

If the number of counter-measures is I , the expected sojourn time of threat j in the whole information security system

$$W_j = \sum_{k=1}^I \prod_{l=1}^k (1 - p_{l-1,j}) W_{kj} \quad (4)$$

where $p_{0j} = 0$ and $W_{kj} = \frac{1}{\mu_{kj}} + P_k(m_k) \cdot \frac{J}{\sum_{j=1}^J \mu_{kj}} \cdot \frac{1}{1-\rho_k}$.

Then the expected sojourn time for an arbitrary threat in the information security system

$$W = \sum_{j=1}^J \left(\frac{\lambda_{1j}}{\sum_{j=1}^J \lambda_{1j}} \right) W_j. \quad (5)$$

4. Numerical Example

If we consider two information security technologies, firewall and IDS, and three kinds of information threats, information theft, denial of service and virus, the information security system consists of following nodes and threats:

- Node 1 ($i=1$): firewall (information security technology for preventive control);
- Node 2 ($i=2$): IDS (information security technology for detective control);
- Node 3 ($i=3$): recovery system for corrective control;
- Threat 1 ($j=1$): theft of proprietary information;
- Threat 2 ($j=2$): denial of service;
- Threat 3 ($j=3$): virus attack.

Suppose values of the parameters m_i , λ_{ij} , μ_{ij} , p_{ij} as in Table 1.

Table 1. Parameter values

Number of units	Arrival rates of threats (per day)	Service rates of counter-measures (per day)	Efficiencies of counter-measures
$m_1 = 1$	$\lambda_{11} = 0.04$	$\mu_{11} = 10$	$p_{11} = 0.57$
$m_2 = 1$	$\lambda_{12} = 0.05$	$\mu_{12} = 10$	$p_{12} = 0.47$
$m_3 = 1$	$\lambda_{13} = 0.13$	$\mu_{13} = 10$	$p_{13} = 0.67$
	$\lambda_{21} = (1 - p_{11})\lambda_{11}$	$\mu_{21} = 10$	$p_{21} = 0.57$
	$\lambda_{22} = (1 - p_{12})\lambda_{12}$	$\mu_{22} = 10$	$p_{22} = 0.40$
	$\lambda_{23} = (1 - p_{13})\lambda_{13}$	$\mu_{23} = 10$	$p_{23} = 0.67$
	$\lambda_{31} = (1 - p_{21})\lambda_{21}$	$\mu_{31} = 0.03$	
	$\lambda_{32} = (1 - p_{22})\lambda_{22}$	$\mu_{32} = 0.08$	
	$\lambda_{33} = (1 - p_{23})\lambda_{23}$	$\mu_{33} = 0.07$	

Then we have $W = 8.3$ days. That is, an arbitrary information threat would wait 8.3 days in the information system of the organization until the information threat is effectively prevented (or detected), or the damage caused by the information threat is recovered.

5. Conclusions

In this paper we suggested performance measures to evaluate the information security systems. If we consider one information security technology, we can evaluate each information security technology. If we consider multiple information security technologies, we can evaluate information security investment portfolios.

If we assume a fixed budget to invest in information security, we can find the optimal investment portfolios, out of various information security counter-measures, to enhance an organization's information security system. We suggest this topic for future research.

Appendix A. Derivation of $\frac{\mu_{1k}}{\sum_{j=1}^J \mu_{1j}}$

$$\begin{aligned}
 P(X_{11} > X_{1k}, X_{12} > X_{1k}, \dots, X_{1J} > X_{1k}) &= \int_{x=0}^{\infty} P(X_{11} > X_{1k}, X_{12} > X_{1k}, \dots, X_{1J} > X_{1k} \mid X_{1k} = x) f_{X_{1k}}(x) dx \\
 &= \int_{x=0}^{\infty} P(X_{11} > x, X_{12} > x, \dots, X_{1J} > x) f_{X_{1k}}(x) dx \\
 &= \int_{x=0}^{\infty} P(X_{11} > x) \cdot P(X_{12} > x) \cdot \dots \cdot P(X_{1J} > x) f_{X_{1k}}(x) dx \\
 &= \int_{x=0}^{\infty} e^{-\mu_{11}x} \cdot e^{-\mu_{12}x} \cdot \dots \cdot e^{-\mu_{1J}x} \cdot \mu_{1k} e^{-\mu_{1k}x} dx \\
 &= \mu_{1k} \int_{x=0}^{\infty} e^{-\left(\sum_{j=1}^J \mu_{1j}\right)x} dx \\
 &= \frac{\mu_{1k}}{\sum_{j=1}^J \mu_{1j}} .
 \end{aligned}$$

References

- [1] Bodin, L.D., Gordon, L.A., and Loeb, M.P. "Evaluating information security investments using the analytic hierarchy process", Communications of the ACM, Vol.48, No.2, pp.79-83, 2005.
- [2] Cavusoglu, H., Mishra, B., and Raghunathan, S., "A model for evaluating IT security investments", Communications of the ACM, Vol.47, No.7, pp.87-92, 2004.
- [3] Cavusoglu, H., Mishra, B., and Raghunathan, S., "The value of intrusion detection systems in information technology security architecture", Information Systems Research, Vol.16, No.1, pp.28-46, 2005.
- [4] Computer Security Institute, CSI/FBI Computer Crime and Security Survey, 2005.
- [5] Gordon, L.A. and Loeb, M.P. "The economics of information security investment", ACM Transactions on Information and Systems Security, Vol.5, No.4, pp.438-457, 2002.
- [6] Kleinrock, L. Queueing Systems, Volume 2: Computer Applications. John Wiley, New York, 1976.