December 2006

A Framework for Assessing IT Security Investment Portfolios

Ram Kumar
UNC-Charlotte

Sungjune Park
UNC-Charlotte

Chandrasekar Subramaniam
UNC-Charlotte

Tae Sung
Chunkbuk Natrional Unviersity

A Framework for Assessing IT Security Investment Portfolios

Ram L Kumar
UNC-Charlotte
rlkumar@uncc.edu

Sungjune Park
UNC-Charlotte
supark@email.uncc.edu

Chandrasekar Subramaniam
UNC-Charlotte
csubrama@email.uncc.edu

Tae-Sung Kim
Chunkbuk Natrional Unviersity
kimts@chungbuk.ac.kr

ABSTRACT

Organizations are faced with different types of information security threats and implement several security technologies to mitigate these security threats. The security technologies vary in their ability to deal with different types of security threats and hence, organizations usually implement a portfolio of security technologies. A key challenge for organizations is to evaluate and determine the value of the counter-measures in the context of these portfolios. *This research develops a framework for systematically evaluating the value of portfolios of different types of security investments given the threats and business environment faced by an organization. The proposed framework builds on the theory of financial asset valuation and develops a simulation model that considers a variety of factors such as type of threat, frequency of arrival, possible damage, and recovery time from damage.*

Key Words: IT Security Portfolio, Business Value of IT Security Portfolio, IT Asset Valuation, Economics of IT Security

INTRODUCTION

Organizations are faced with different types of information security threats. Virus attacks and denial of service attacks alone resulted in about $81 million in losses in 2004 for organizations, according to a survey by CSI/FBI (Gordon et.al., 2004). In response to these threats and attacks, organizations continue to implement several counter-measures, including anti-virus software, firewalls, intrusion detection and/or prevention, and encryption (of files and of data in transit). A key challenge for organizations is to evaluate and determine the economic consequences of the security threats and counter-measures. Most organizations implement a portfolio of the security technologies and there is relatively little research on the economic benefits of portfolios of security technologies, which recognizes the differences and interrelationships between benefits provided by different technologies in the portfolio. *Our research develops a framework for systematically evaluating the value of portfolios of different types of security investments. The framework builds on the theory of financial asset valuation and develops a simulation model that considers a variety of factors such as type of threat, frequency of arrival, possible damage, and recovery time from damage.*

OVERVIEW OF IS SECURITY THREATS AND TECHNOLOGIES

A security threat refers to the attempt made to compromise an information system to exploit the systems vulnerability. An attack is the materialization of the threat or the actual exploitation of an IS security vulnerability[1]. A CSI/FBI study has identified different types of attacks on organizational information systems, including virus and worms, insider abuse of network access, laptop theft, denial of service, system penetration, unauthorized access of information system resources or data, and theft of proprietary information (Gordon et.al., 2004). Another study found that theft of proprietary/confidential information, virus attacks, and denial of service are the three most important security threats to information systems (Farahmand et al., 2003). Table 1 summarizes the impact of these attacks on organizations. The loss suffered by a firm related to the security attack can be in the form of loss of confidential information, faulty decisions based on altered data, or loss of business from denial of service (Gordon and Loeb, 2002).

[1] Even though a threat is, strictly speaking, different from an attack, we have used the terms interchangeably in our paper.

IS security threat	Impact on organization
Theft of proprietary/ confidential information	Loss of confidence by customers and business partners Loss of business Financial liability
Virus and worms	Loss of productivity Disruption of business operations
Denial of service	Loss of business
Physical damage / Sabotage	Disruption of business operations Loss of business

Table 1. Major types of security attacks and their organizational impacts

There are many security technologies used by organizations as counter-measures to address the IS security threats. The security technologies are constantly evolving in response to the ever-changing nature of the threats and the novel methods adopted by the threat agents. However, based on studies by several IS security researchers and organizations such as CERT and CSI, we have identified the major IS security technologies (ISST) and their characteristics in Table 2.

LITERATURE REVIEW

Our research builds on two streams of literature in the IS area. The first stream relates to the value of IT investments. Studies that have analyzed the business value of IT in organizational contexts have emphasized that the extent of IT use and the context in which IT is used are major determinants of IT value (Mukhopdhyay Kekre and Sundar, 1995, Fan, Stalhert and Whinston 2000, Devaraj and Kohli, 2003, Kumar 2004). Hence it is important to consider the context in which ISST are used in order to determine their value.

The second stream relates to information security investments, including economic models. Gordon and Loeb (2002) consider an economic model that examines how the vulnerability of information and the potential loss from such vulnerability affects the optimal resources to invest in security. A economic model of intrusion detection systems by Cavusoglu et. al., (2005) shows that with optimally configured IDS, the value from such a system is strictly non-negative and this configuration always deters hackers. The economic views also recognize that when using security technologies, organizations may have to consider trade-offs and conflicts among their security goals and it is necessary to evaluate any security portfolio in terms of the corporate IS security priorities (Gordon and Loeb, 2002). Our model specifically considers a portfolio of security investments and the effectiveness of different portfolios of IS security technologies. We describe our model in the next section.

UNDERSTANDING DIFFERENT TYPES OF ISST AND THEIR RELATIONSHIP TO BUSINESS VALUE

Consider a hypothetical scenario where an organization has no ISST. We use this scenario as a base case to illustrate the value added by different types of ISST. The "value" of the organization's IT infrastructure and applications (ITIA) can be denoted by the NPV generated by IT applications that the infrastructure supports. The value of ITIA is affected not only by the type of ISST, but also by the manner in which it is used. For example, an infrastructure supporting e-commerce sales transactions on the Web is more valuable when the number of users is high. The value of the organization's infrastructure and applications varies over time, due to variations in factors such as number of users and number of transactions using it. *Hence we can model IT infrastructure and applications value IV as a function of usage* (*the number of transactions as well as the value of each transaction*).

Technology	Description	Product Examples	Some issues to consider
Firewall	Hardware or software that is programmed to filter the information coming through the Internet connection into a protected network. A fire wall monitors and regulates network traffic and data flows based on categorization of information risk. Three methods used by firewalls are packet filtering, proxy service or stateful inspection	SmoothWall Corporate Firewall, Sygate Firewall, Netop Desktop Firewall, Kerio WinRoute Fire wall	Protects from information theft and denial of service attacks
Anti-virus products / services	Software that protects network from known virus and worms; Maybe combined with a comprehensive management solution from the anti-virus vendor, including early warning services	Symantec Integrated Security, McAfee Anti-Virus	Protects against virus and worms
Encryption	Encryption generally involves the use of a key to encrypt data or message before transmission. The receiver uses the key to decrypt the data or message. Public-key encryption uses a combination of a private key (known to the decoder only) and a public key (which is used to encrypt).	PGP	Theft
IDS	Hardware and/or software systems that monitor the events occurring in a computer system or network, analyze them for signs of security problems, and warn security experts about suspected intrusions (Cavusoglu et al., 2005). Anomaly detection builds profiles of normal activities and alerts when monitored activity deviates from normal. Misuse detection constructs patterns of known attacks and alerts when monitored activity matches known pattern (Ning and Xu, 2004)	Snort, DShield	Intrusion detection during early stage of attack can lead to false alarms and make proactive defense actions very expensive (Liu et al., 2006)

Table 2. Major countermeasures to combat security threats

In general, *IV* can be modeled as a time-dependent variable which follows a certain pattern, i.e. a stochastic process (Kumar, 2004). Let IV_t be the NPV of the infrastructure and applications at time *t*. IV_t varies over time due to changes in the usage of applications supported, addition of new applications, environmental factors such as the economy and competition, addition of new applications, and other factors.

Following Kumar (2004), the change in IV_t can be considered as being made up of three types of changes. Each of these changes can be positive or negative. The first type of change, termed the ***drift*** in value is a *small change in value that could accumulate over time to form a larger change in value*. An example of such a change would be an increase in rate of usage of an e-commerce site. The second type of change, termed ***noise,*** is a "*small instantaneous perturbation in value that does not exhibit a long-term pattern*". An example of such a change would be random daily fluctuations in usage. As in the case

of stock prices (Press, 1969), the Weiner Stochastic Process is used to model the short-term perturbations in IV_t. The third type of change, termed ***jump*** is a "*sudden, relatively large change in value*." An example of such a change would be a sudden spike in number of transactions during the closing of an auction e-commerce site, or due to the addition of a new type of revenue earning application on the web site. It is important to realize that these three parameters could be positive or negative. For example, certain applications could have a negative trend in usage or a software glitch could result in a negative jump. Figure 1 illustrates the variation of IV_t as a function of these three types of changes.

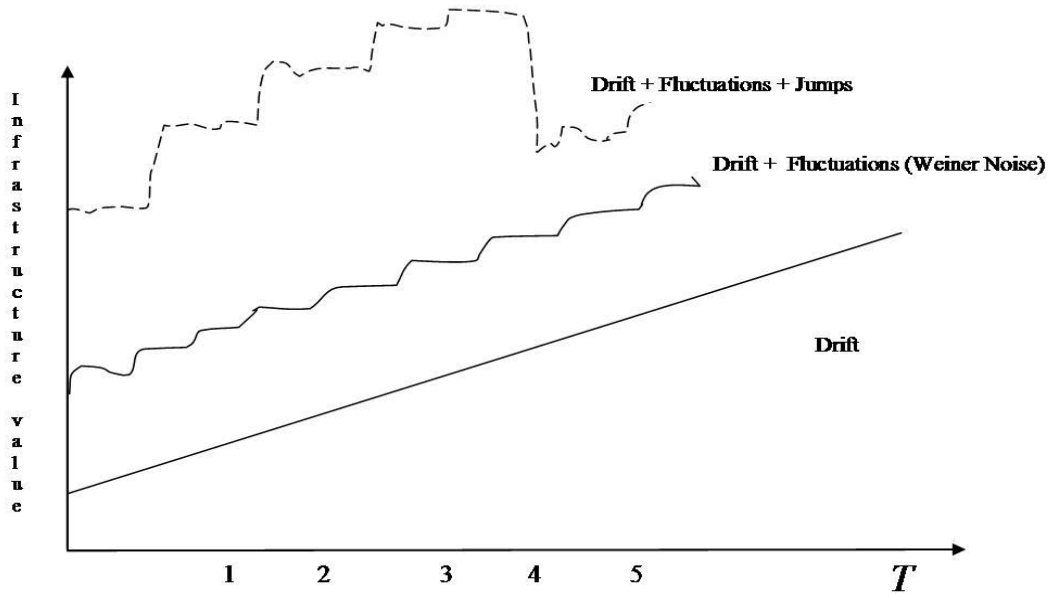

Figure 1. Components of changes in IV_t

Arrival of jump events can be modeled to follow Poisson process $A_k(t)$ with arrival rate λ_k where *k* denotes the type of jump. For any jump event of type *k*, there will be costs associated with responding to the event (c_k) and benefits resulting from responding to the event (b_k). The net effect of these costs and benefits (a_k) is a positive or negative jump in IV_t and may be modeled to follow a lognormal distribution for each jump event *k*.

Jump Event (k)	Benefit	Cost
Installation of a new application	Value generated by the new application	Cost of installing the new application on the infrastructure
Integration of critical applications	Additional value generated by the integration	Cost of integration
Power Failure		Loss in value due to business disruption
Denial of Service Attack		Loss in value due to system downtime
Hacker attack		Loss in value due to negative publicity, and potential liability claims
Theft of information		Loss in value due to business disruption, loss of current and future business, and potential liability claims

Table 3. Illustrative events affecting value of an IT infrastructure

It is important to note that in Figure 2, we have assumed that the effect of ISST is to reduce the magnitude of negative jumps. In general ISST can enhance infrastructure value in one or more of the following ways:

(i) By decreasing jump sizes for negative events;
(ii) By decreasing the arrival rate of negative events (Figure 3);
(iii) By reducing the time to recover (or by increasing the recovery rate) from negative events (Figure 4); and
(iv) By providing early warning of possible security threats and thus, increasing the time to react to security threats.

Table 3 illustrates some events that may occur as well as the associated costs and benefits. *Initially, it is assumed that the infrastructure includes a basic ISST portfolio (BISST).* Figures 2 and 3 illustrate the variation of IV_t resulting from the events described in Table 3 for two ISST portfolios: a basic portfolio (BISST), and an advanced portfolio (AISST). ISST is assumed to have no effect on installation of new application and integration of critical application. However, for the security-related events, ISST reduces the magnitude of negative jumps. Thus the value added by investing in AISST instead of BISST is the difference in areas between the two curves (AISST, and BISST) for some planning horizon T.

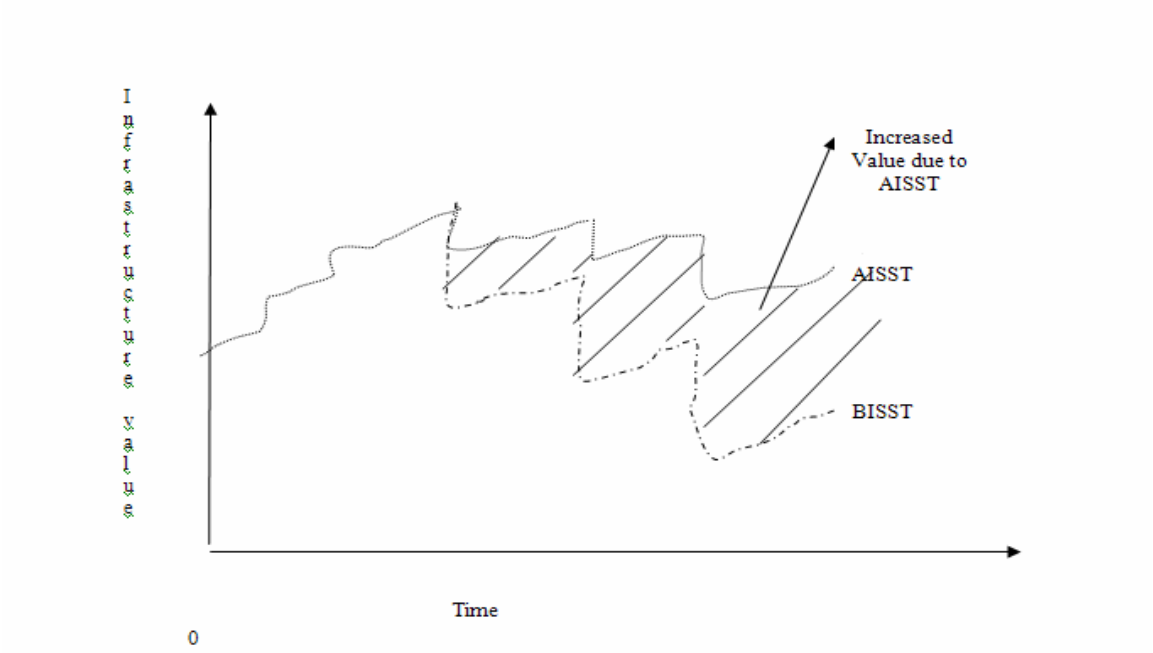

Figure 2. Increased value due to an AISST that reduces the magnitude of negative jump events compared to a BISST

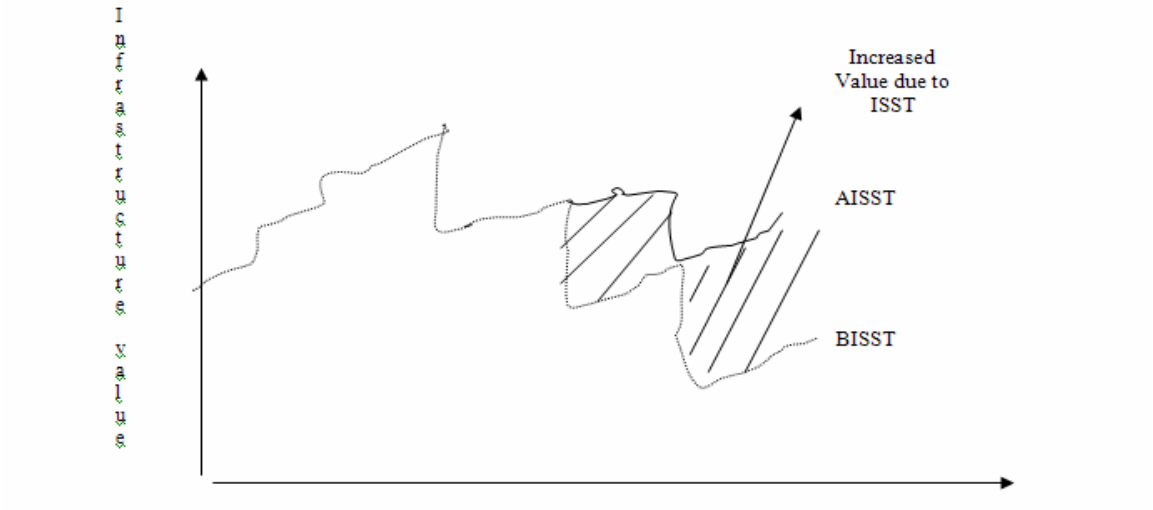

Figure 3. Increased value due to an AISST that reduces the arrival rate of negative events compared to a BISST

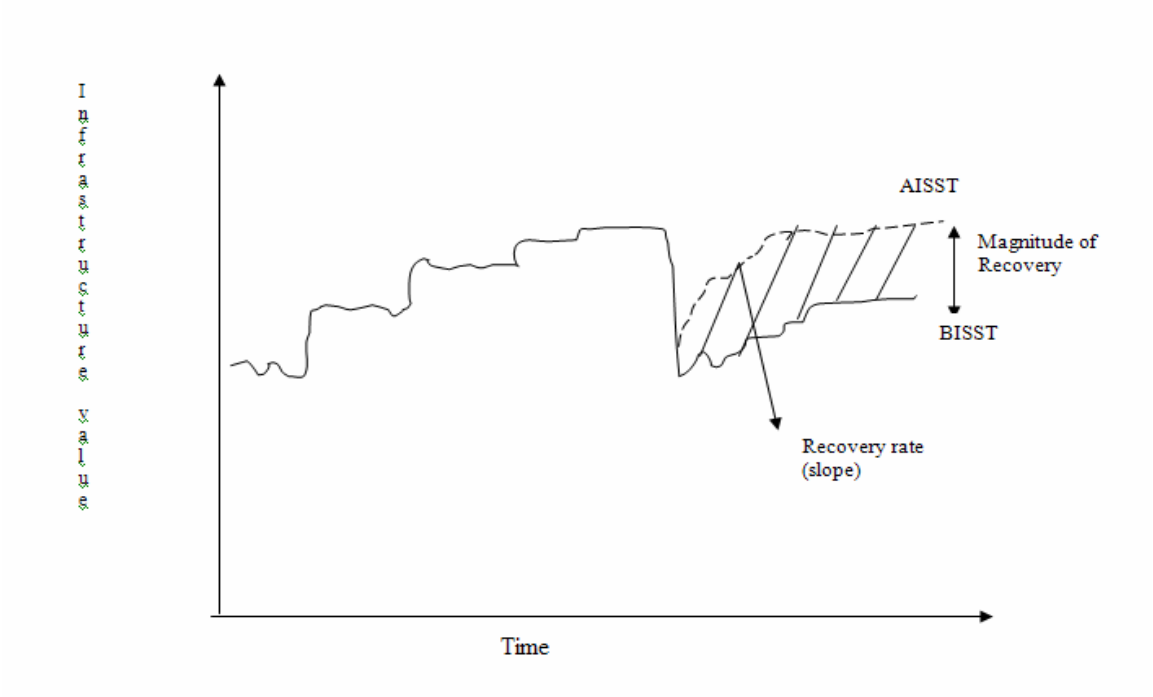

Figure 4. Increased value due to an AISST that increases the recovery rate and magnitude of recovery from negative events compared to a BISST

Having time to react to a security attack is very useful for organizations as it can help in preparing and prioritizing the security defenses. These early warnings can come from the ISST (for e.g., an IDS warning) or from the attack and response timeline of three types of technologies – technologies that aid in detecting attack (e.g. intrusion detection systems), technologies that aid in detecting and recovering from an attack (e.g. anti-virus systems), and technologies that are only used for recovery once an attack has happened (e.g. back-up and recovery systems). We can therefore envisage the timeline from the occurrence of an attempted attack to the time the system is fully recovered as shown in figure 5.

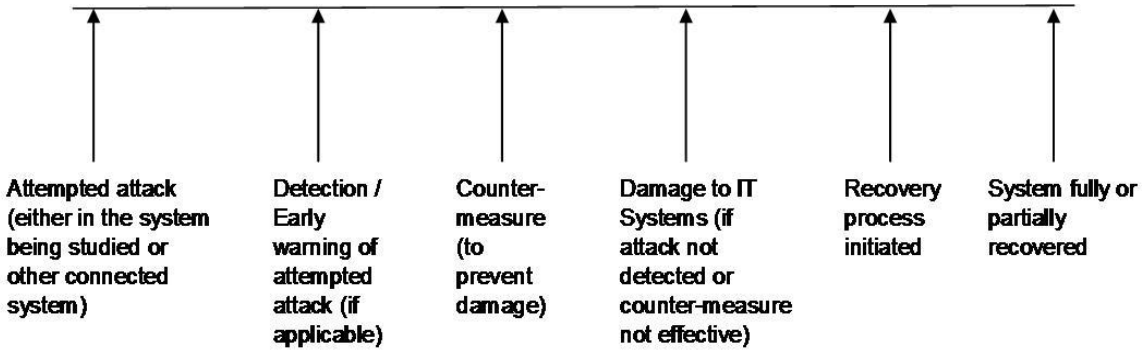

Figure 5. Timeline of security attack and ISST response

Each type of ISST can have different types of impact on the Attack-Recovery timeline. Table 4 below illustrates the types of effects that common types of ISST can have. An ↑ denotes a positive effect, and a ↓ denotes a negative effect on each of the parameters in the column headings.

	Jump magnitude	Arrival rate	Recovery rate	Reaction time window
Firewall		↓		
Anti-virus products / services		↓	↑	↑ (with early warning service)
Encryption	↓	↓ (announcing encryption is a possible deterrent)		
Intrusion Detection System	↓			↑

Table 4. Illustration of the different effects of ISST

SIMULATION MODEL

Because of the interactions and interdependences between threats, countermeasures, and other operating environments, which analytical models cannot fully address, a simulation model has been developed. The simulation model addresses four types of effects (See Table 4) associated with different business environments, combinations of security threats, and ISST portfolios.

We use two types of parameters in our simulation. The environmental parameters include those associated with the business environments and threats as listed in Table 5. For example, lifetime of ISST (*T*), drift rate (α), short-term noise representing volatility of IT infrastructure value (dz_t), arrival rates of jumps (λ_k), and means and variances of jump magnitudes (a_t) are considered environmental parameters. The other type of parameters is related with effects of threats: frequency of threat arrival (λ_j), amount of damage (θ_j), time required to recover from damage *j* (τ_j), and amount of post-recovery damage (ρ_j). The values of these parameters are not independent of business environments and thus should be considered accordingly. For this reason, we use beta distribution for post-recovery damage (ρ_j) in order to incorporate IT managers' insights and experiences in their business environment. The time required to recover from damage is assumed to follow exponential distribution, which is a special case of Erlang distribution widely used for service time in queuing systems.

In addition to the environmental parameters, the simulation requires parameters associated with countermeasures as well for evaluation of ISST portfolios. These parameters mostly represent the effectiveness of countermeasures on expected damage, recovery time, and recovery magnitude. Since the effectiveness of counter-measures is also experiential, we assume that these parameters follow beta distribution as well. The simulation parameters and their distributions are summarized in Table 5.

An object oriented programming language Java was used in order to build a model such that events such as jumps, damages, and recoveries are treated as objects with properties such as type, magnitude, arrival time, and the like. Although the conceptual model above illustrates various events (arrival, detection, and prevention of threats; and arrival and recovery of damages), the events considered in the simulation are arrivals of damages resulting from arrivals of threats and countermeasures' responses. From the assumption that arrival process of threats is a Poisson process with λ_j, we can derive that a successful threats that are not prevented by counter-measures follow a Poisson process with $\lambda_j \left(\prod_j p_{ij} \right)$. Furthermore, arrivals of damages caused by successful threats follow the same Poisson process with $\lambda_j \left(\prod_j p_{ij} \right)$ because the departure process of M/G/1 queuing system is also a Poisson process, a property known as PASTA (Poisson Arrivals See Time Average) (Wolff 1982). Therefore, our simulation model does not take into account detection and response activities by countermeasures during the time between the arrival of a threat and its damage.

Using common random numbers (Law and Kelton 1991), each ISST portfolio is subjected to the same pseudo-random conditions in terms of threat arrivals. This approach results in smaller variance and allows fewer observations for statistical significance tests such as t-test or analysis of variance.

CONCLUSION AND CONFERENCE PRESENTATION

Simulation results illustrate the relationships between an organization's business environment, the threat environment in which it operates and characteristics of its ISST. These results and related managerial and research implications will be presented at the conference.

Type	Parameter	Random Variable and/or Underlying Stochastic Process	Distribution Used in Simulation Model
Business Environment (fixed)	T : lifetime of ISST; simulation period.	Constant	
	α : drift rate	Constant	
	σ_z : instantaneous variance	dz_t, Weiner	Normal distribution
	λ_k : arrival rate of jump type k	$A_k(t)$: Poisson	Exponential distribution
	μ_k, σ_k : mean and s.d. of jump k	a_k	Lognormal distribution
Threat Environment (fixed)	λ_j : arrival rate of threat type j	$T_j(t)$: Poisson	Exponential distribution
	μ_j, σ_j : mean and s.d. of damage j	θ_j	Lognormal distribution
	s_j : mean time required to recover from damage j	τ_j	Exponential distribution
	ρ_j^a, ρ_j^b, ρ_j^m : optimistic, pessimistic, and most likely estimates of post-recovery damage.	ρ_j	Beta distribution
Counter-measure effectiveness (variable)	p_{ij} : Ineffectiveness of counter-measure i on threat j	X (1 or 0)	Bernoulli distribution
	q_{ij}^a, q_{ij}^b, q_{ij}^m : optimistic, pessimistic and most likely estimates of effect of counter-measure i on θ_j	q_{ij}	Beta distribution
	s_{ij}^a, s_{ij}^b, s_{ij}^m : optimistic, pessimistic and most likely estimates of effect of counter-measure i on τ_j	s_{ij}	Beta distribution
	r_{ij}^a, r_{ij}^b, r_{ij}^m : optimistic, pessimistic and most likely estimates of effect of counter-measure i on ρ_j.	r_{ij}	Beta distribution

Table 5. Simulation parameters and distributions used.

REFERENCES

1. Cavusoglu, H., Mishra, B. and Raghunathan, S. (2005)The Value of Intrusion Detection Systems in Information Technology Security Architecture, *Information Systems Research*, 16, 1, 28-46.

2. Conrad, J.R. (2005) Analyzing the Risks of Information Security Investments with Monte-Carlo Simulations, *IEEE Workshop on the Economies of Information Security*, http://infosecon.net/workshop/pdf/13.pdf , retrieved May 1, 2006.

3. Devaraj, S. and Kohli, R. (2003) Performance Impacts of Information Technology: Is Actual Usage the Missing Link? *Management Science*, 49, 3, 273-289.

4. Farahmand, F., Navathe, S.B., Sharp, G.P. and Enslow, P.H. (2003) Managing Vulnerabilities of Information Systems to Security Incidents, *5th International Conference on Electronic Commerce*, September 30-October 3, Pittsburgh, PA, USA, ACM Press, 348-354

5. Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Richardson, R. (2004) Ninth Annual CSI/FBI Computer Crime and Security Survey, *Computer Security Institute*, http://www.gocsi.com, retrieved May 1, 2006.

6. Gordon, L.A. and Loeb, M.P. (2002) The Economics of Information Security Investment, *ACM Transactions on Information and System Security*, 5, 4, 438-457.

7. Kumar, R. (2004) A Framework for Assessing the Business Value of Information Technology Infrastructures. *Journal of MIS*, 21, 2, 11-32.

8. Press, J.S. (1967) A Compound Events Model For Security Prices. *Journal of Business*, 40, 3, 317-335.