View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by AIS Electronic Library (AISeL)

Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2010 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

2010

Optimal Investment in Information Security: A Business Value Approach

C. Derrick Huang
Florida Atlantic University, dhuang@fau.edu

Follow this and additional works at: http://aisel.aisnet.org/pacis2010

Recommended Citation
Huang, C. Derrick, "Optimal Investment in Information Security: A Business Value Approach" (2010). *PACIS 2010 Proceedings*. 45.
http://aisel.aisnet.org/pacis2010/45

This material is brought to you by the Pacific Asia Conference on Information Systems (PACIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in PACIS 2010 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

OPTIMAL INVESTMENT IN INFORMATION SECURITY: A BUSINESS VALUE APPROACH

C. Derrick Huang, Department of Information Technology and Operations Management, Florida Atlantic University, Boca Raton, FL, U.S.A., dhuang@fau.edu

Abstract

With increasing level of security threats and constant budget limitations, it is critical for a company to know how much and where to invest in information security. To date, all of the studies—academia or practitioner—focus on risk reduction as the primary effect of security investments, assuming that they generate no direct business benefits. However, some potential business values such as brand reputation and data stability are not only real but also quite important. This study addresses related research questions and extends the existing model to take into account direct business benefits in optimizing security investments, filling a significant research gap. As such, this research makes contribution to both theory development in information security management and management implications in practice.

Keywords: IT security, information security investment, optimal investment, business value

1. INTRODUCTION

Managing information security has become an integral part of any company's day-to-day operations. In the ten year period leading to 2003, the number of security incidents reported to CERT increased from 1,334 to 137,529 per year (CERT, 2006). Such incidents range from those by hackers with benign consequences, to attacks aimed at stealing valuable information, to cyber-terrorism. To protect against such risks, organizations are investing heavily in information security-related products and services, in addition to the countless manpower and management attention dedicated to protecting the data and systems and recovering from virus infections and occasional breaches (Gordon et al., 2006). Given the high cost of information security and the fact that a "completely secure organization" is an insurmountable, if not impossible, goal in today's networked economy, it is only natural for decision makers to wonder if their investments are made wisely and effectively. It is therefore important for decision makers to be able to determine the *optimal* amount of investment, and a number of studies have been devoted to address this issue based on economic cost-benefit analysis (Gordon and Loeb, 2002; Hauske, 2006; Huang et al., 2008). This approach, though widely adopted for evaluating IT investments, is complicated by the fact that the "return" of security investment does not come from increased revenues or decreased costs like other IT investments do, but from reduced security risks that a firm is facing (Alter and Sherer, 2004). As a result, it is difficult for a decision maker to employ such economic models to determine if the level of information security investment of her company is appropriate, because its intended outcome is "nothing happened." This project is designed to fill the research gap by building a business-value model for evaluating optimal level of security investment that considers not only the risk reduction aspect but also the business benefits of such investments.

2. RESEARCH BACKGROUND AND RESEARCH QUESTIONS

The research stream on the optimal level of information security investment began in the early 2000s. In their seminal paper, Gordon and Loeb (2002a) analyze the economics of security investment for a risk-neutral firm by comparing the cost of the investment and the potential loss caused by possible security breaches. They find that the optimal security investment would be far less than (with a theoretical maximum of 36.8% of) the potential loss if a security breach does happen, and that the optimal security investment does not necessarily increase with system vulnerability. In extending the Gordon and Loeb model, Huang et al. (2008) adopt the expected utility theory to study the behavior of a risk-averse decision maker and find that there exists a minimum potential loss for non-zero optimal information security investment; above that minimum, optimal investment increases with potential loss. In addition, contrary to the risk-neutral case, a risk-averse decision maker may continue to invest in information security until the spending is close to (but never exceeds) the potential loss.

After the amount of investment is determined (by optimization, budget, or other constraints), a firm needs to decide what security measures to invest in. Often, selection of the right investments is aided by traditional management tools as cost-benefit analysis (Gordon and Loeb, 2006) and financial analyses based on such measures as return on investment (ROI), net present value (NPV), and internal rate of return (IRR) (Pursor, 2004, Gordon and Loeb, 2002b). Studies have proposed other decision analysis methodologies for selecting the right security investments. For instance, analytic hierarchical process (AHP) employs pair-wise comparisons among different security technologies to determine the priority of implementation (Bodin et al., 2005). Arora et al. (2004) propose to value security investments by associating bypass rate with each of the security technologies adopted at a firm. Alternatively, the issue of selecting and prioritizing security technologies can be treated as optimizing the allocation of the limited security investment. Taking such an approach, Huang et al. (2006) propose an analytic model for security investment allocation that considers simultaneous attacks from multiple threat agents with distinct characteristics. Their analysis shows that a firm is better off allocating most or all of the investment to defending against one type of attack when its security

budget is small. Further, a firm should focus on technologies against targeted attacks when its information systems are highly connected.

A common modelling technique adopted by all of the studies in this body of research is the traditional decision analysis by comparing the economic cost and benefit of information security investments. The benefits of such investments mainly come from the reduction of a firm's security risks, which is formulated as security risk = (likelihood of loss event) * (cost of loss event) (Schechter, 2005). This approach, though widely adopted, implicitly assumes that investments information security does not bring about direct business benefits such as revenue generation or cost savings. This assumption seems plausible at first, because the main objective for security measures is to prevent adverse event from happening. Recent studies, however, shed light on possible business values that such investments would bring to an organization. It is found that, for instance, IT security can enhance a company's knowledge management process (Jennex and Zyngier, 2007) and instil confidence in its reputation and brand (Emory, 2007). Further, information security efforts improve and sustain a company's resiliency, allowing it to better adopt to ever changing risk environment (Daneva, 2006) and, thus, potentially advancing its competitive advantage (Wang, 2004). To address this gap, the current project takes a business-value approach to address the following issues:

(i) How can business benefits from information security be formulated?

(ii) How can both risk reduction and business benefits be accounted for in optimizing a firm's information security investment?

(ii) How does the optimal level of investment based on business value behave with respect to environmental parameters such as connectivity, potential loss, and attack probability?

3. BASE MODEL—RISK MANAGEMENT APPROACH

The commonly adopted model (Huang et al., 2008; Gordon and Loeb, 2002a) examines the attack based on the breach probability and expected loss. Security adversaries generate attacks on the information systems with a threat probability t. In turn, the security property of the information systems is determined by the system vulnerability and security investment. The system vulnerability, v, is assumed to be a direct result of the topology and connectivity of the firm's information systems: The more accessible and connected the systems, the more intrinsically susceptible they are to attacks. To protect against the system vulnerability being exploited by threat agents, the firm invests S in security measures. The probability of a security breach to occur can then be considered as a function of the behavior of the attack agents, as described by the threat probability, and the security property of the information systems, which, in this model, is determined by the system vulnerability and investments in security measures. In other words, the breach probability p can be written as the following:

$$p = p(t, v, S). \tag{1}$$

For simplicity, we require that both t and v to be between 0 and 1. Note that for any given system, the higher the security threat and the more susceptible to attacks, the higher breach probability; that is, both $\frac{\partial p}{\partial t} \geq 0$ and $\frac{\partial p}{\partial v} \geq 0$. Further, the effect of the security investment is to reduce the breach probability, or

$$\frac{\partial p}{\partial S} \leq 0. \tag{2}$$

We assume that this reduction is governed by the law of diminishing return, which implies that

$$\frac{\partial^2 p}{\partial S^2} \geq 0. \tag{3}$$

We also require the following boundary condition $p(t, v, 0) = tv$. That is, when the firm does not make any security investment, the breach probability is solely determined by and can be described as a product of the threat and the intrinsic system vulnerability.

A common definition of risk is the combination of the likelihood and the consequence of a specified hazard being realized (Schechter, 2005). The security risk R the firm faces can therefore be written as

$$R = p\mathrm{L}, \tag{4}$$

where L is potential economic loss caused by a security breach. For this model, one can make the simplifying assumption that L > 0 is a fixed amount, as estimated by the firm based on the type of attack. From the boundary condition $p(t,v,0) = tv$, the security risk a company faces when no investment is made is tvL. To protect against the attack, the firm makes investment S to reduce the breach probability such that the information security risks is reduced by $\Delta R = (tv - p)\mathrm{L}$. In other words, the net benefit Π of the security investments would be

$$\Pi(S,t,v) = (tv - p)\mathrm{L} - S. \tag{5}$$

The task of optimizing the security investments is to maximize their benefits by setting the first-order partial differentiation of Π in (5) with respect to S to 0; that is, $\frac{\partial \Pi}{\partial S} = 0.$ Note that this operation indeed yields maximum, not minimum, of Π:

$$\frac{\partial^2 \Pi}{\partial S^2} = -\frac{\partial^2 p}{\partial S^2}\mathrm{L} \le 0, \tag{6}$$

because of (3).

To further account for breach probability p, a derivation that has its root in scale-free networks is adopted (Albert et al., 1999; Faloutsos et al., 1999; Kumar et al., 2000). It has been shown that the connectedness of the Internet and the worldwide web resembles that of a scale-free, small-world network, distinguished by a limited number of highly connected nodes (called "hubs") as well as by its structural independence of the system's size N (Barabási and Albert, 1999; Watts and Strogatz, 1998). In a scale-free network, the probability that a node connects with k other nodes is roughly proportional to $k^{-\gamma}$, where γ is between 2 and 3 for most real networks such as the Internet (Barabási and Albert, 1999).

To examine how the scale free network can shed light on the directed attacks, the case that an epidemic event starts spreading in a scale-free network (Chang and Young, 2005; Pastor-Satorras and Vespignani, 2001) is used. The rate of epidemic spreading, λ, is determined by r, the infection rate of a previously uninfected node if it is connected to an infected one, and δ, the remediation rate of an infected node:

$$\lambda = \frac{r}{\delta}. \tag{7}$$

Let $P_k(t)$ denote the relative density of infected nodes with k connections—that is the probability that a node with k connections is infected—at time t. The mean field rate equation gives (Pastor-Satorras and Vespignani, 2001)

$$\frac{\partial P_k(t)}{\partial t} = -P_k(t) + \lambda k[1 - P_k(t)]\Theta(\lambda), \tag{8}$$

where $\Theta(\lambda)$ is the probability that any given connection points to an infected node, which can be given in the lowest order of λ (Chang and Young, 2005):

$$\Theta(\lambda) = \frac{e^{-\lambda n}}{\lambda n}, \tag{9}$$

where n is the minimum number of nodes available for connection in such a network. Solving for P_k in a steady state (i.e., $\partial P_k(t) \big/ \partial t = 0$), one gets

$$P_k = \frac{k\lambda\Theta(\lambda)}{1 + k\lambda\Theta(\lambda)}. \tag{10}$$

When averaging P_k over k, one gets the average infection probability of any node in the network (Pastor-Satorras and Vespignani, 2001):

$$P = ce^{-\frac{1}{\lambda n}}, \tag{11}$$

where c is a normalization constant.

To extend this result to security investment of the firm's information systems, it is assumed that the firm's information systems can be represented as a node in such a network. Further, it is assumed that the effect of security investment S can be shown in the reduction of the infection rate λ in (9). λ and S satisfy certain boundary conditions. First, the attack would be spread freely to the node without any security investment; in other words, $\lambda = 1$ when $S = 0$. Second, any finite security investments, no matter how large, would never be able to fully block all attacks; in other words, $\lambda \to 0$ only when $S \to \infty$. Without loss of generality, a linear inverse relationship between security investment and infection rate can be used. Such relationship with the above boundary conditions can be expressed in the following manner:

$$\lambda \equiv \frac{1}{\kappa S + 1}, \tag{12}$$

where κ, normalized to between 0 and 1, is a scaling factor for S: The higher the κ, the greater reduction of the infection rate for any given security investment S.

The next set of observations is on the system vulnerability v. Note that since v represents the connectivity of the information systems in question, v would be strictly increasing in n, which represents the extent of connections in such a scale-free network. Further, when $n = 0$, $v = 0$. On the other hand, $v \to 1$ when $n \to \infty$; that is, the systems are highly vulnerable to the epidemic, or security attacks in our case, when they are completely open. Without loss of generality, the following relationship between c and n that satisfies all the above conditions is assigned:

$$v \equiv e^{-\frac{1}{n}}. \tag{13}$$

Lastly, note that the level of threat from attacks is not explicitly considered in (11), which can be accounted for by multiplying (11) with the attack probability t. With this modification, (12) and (13), and adjusting the normalization constant β to reflect the boundary condition $p(t, v, 0) = tv$, one finds that the breach probability for an opportunistic attack can be written as:

$$p = t \cdot P = t \cdot \left(e^{-1/n} \right)^{1/\lambda} = tv^{\kappa S + 1}. \tag{14}$$

Substituting (14) into (5) and rearranging the terms, one gets

$$\Pi(S, t, v) = tvL(1 - v^{\kappa S}) - S, \tag{15}$$

which is the base expression governing the net benefit of security investment amid targeted attacks. All the existing studies in the stream of economic analysis of information security investment research, including Gordon and Loeb (2002a), Hauske (2006), Huang et al. (2006), and Huang et al. (2008), are based on (15) or its variations.

4. EXTENDED MODEL—BUSINESS VALUE APPROACH

In this project, the existing research stream is extended to consider the business value as the basis for security investment. We posit that, in addition to reducing security risks, as represented in $\Delta R = (tv - p)\mathrm{L}$, the security investment S also generate direct business benefits, be they competitive advantage, customer trust, brand loyalty, or some other form, or a combination of them. Let B denotes such business benefits generated from firm's information security, then (15) can be modified as follows:

$$\Pi = B + tvL(1 - v^{\kappa S}) - S, \tag{16}$$

With the addition of the business benefits function, (16) represents the total business value of information security investment that firm is making. To find the optimal level of investment, one can set the derivative of the business value (16) with respect to S to zero:

$$\left.\frac{\partial \Pi}{\partial S}\right|_{S=S^*} = \left.\frac{\partial B}{\partial S}\right|_{S=S^*} - t\kappa(\ln v)Lv^{\kappa S^* + 1} = 0. \tag{17}$$

A further check shows that $\frac{\partial^2 \Pi}{\partial S^2} \le 0$ when $\frac{\partial^2 B}{\partial S^2} \le 0$ (see (i) below), and S^* is indeed the solution that maximizes $\Pi(S,t,v)$. Therefore, once the explicit form of B is known, one can use equation (17) to solve for S^* as the optimal level of security investment that maximizes a firm's business value.

The key to successfully take this business value approach is to identify the properties and, ideally, the appropriate functional forms of B. To start with, note that B depends on both the level of investment and the connectivity of the particular business network; in other words, $B = B(v, S)$. Further, the function B has to satisfy the following properties:

(i) Business benefits, which are derived from information security, need to be an increasing function of security investment with diminishing importance. In other words,

$$\frac{\partial B}{\partial S} \ge 0, \frac{\partial^2 B}{\partial S^2} \le 0 . \tag{18}$$

(ii) Business benefits derived from security investment should be higher when the firm's connectivity is higher:

$$\frac{\partial B}{\partial v} \ge 0 . \tag{19}$$

(iii) When the firm is not connected to any other information systems, its vulnerability is zero, and so are the business benefits for any security investment:

$$\lim_{v \to 0} B(v, S) = 0, \forall S . \tag{20}$$

(iv) When the firm's vulnerability is very high, there is a finite limit of business benefits that can be achieved no matter how much investment is made to protect its information security. In other words,

$$\lim_{S \to \infty} \lim_{v \to 1} B(v, S) = \hat{\mathrm{B}} < \infty . \tag{21}$$

An initial examination, taking into account the above constraints, show that the behavior of an S-curve may be a reasonable form for B, suggesting a Fisher-Pry function or a Gumpertz function. However, further research is need to verify and validate such initial observations, as the proper form of B is critical to the behavior of S^*, the optimal level of investment.

5. PROJECT STRUCTURE

This project is well underway, with all the mathematical modelling done. The following describes the next steps to complete this project:

5.1 Determination of the properties and forms of business benefits function

Because the function B cannot be found in existing literature, it will have to be defined based on available theories, related studies, existing data, and simulation. We will employ various theoretical forms of B (S-curve functions included), run simulation, and compare the functional behavior with data presented in studies such as those by Daneva (2006), Martin (2006), and Jennex and Zyngier (2007). We have also recruited two local firms to provide me with some operational data and to examine the results critically.

5.2 Analysis of the optimal investment

With B defined, we can solve for optimal investment S* in (17). We can then analyze the behavior of the optimal solution with respect to key parameters such as firm's connectivity, attack probability, effectiveness of security measures, and potential loss due to security breaches. Such analyses would produce rich theoretical and practical insights into how firms should decide on security investments under various conditions. (If no closed form of S* can be obtained, one can use implicit function and simulation to obtain such insights.)

5.3 Validation of model and analysis

Validation is a nontrivial, yet important, step of research based on analytics. For the current project we will use the aforementioned local firms as case studies to compare their experience with the project result. Simulation of the optimal investment with respect to different environmental parameters will be produced for such examinations, and the comparison results will be reported in the final paper.

6. CONTRIBUTION

This study extends the current research stream of the economics of information security investment by taking the business value approach to determining a firm's security investment. In doing so, it make theoretical contribution to the research stream, alleviating the limitation on all the studies thus far to consider risk and risk reduction as the only economic impact of security investment on a firm's business. In addition, by explicitly accounting for the business benefits function, the formulation would provide a baseline for the future research on such economic analysis of information security investment. In practice, the results would offer insight into the behavior of optimal investment with respect to various environment parameters, assisting practitioners in making decisions on how much and where to make investments to protect firm's information security while increasing the business values.

References

Albert, R., Jeong, H, and Barabási, A.-L. Diameter of the world-wide web. Nature, 401 (1999), 130-131.

Barabási, A.-L., and Albert, R. Emergence of scaling in random networks. Science, 286 (1999), 509-512.

CERT. (2006) CERT/CC Statistics 1988-2006. 2004. CERT Coordination Center. Available online at http://www.cert.org/stats/cert_stats.html. Last accessed on April 28, 2006.

Chang, D.B., and Young, C.S. Infection dynamics on the Internet. Computers & Security, 24 (2005), 280-286.

Cremonini, D., and Nizovtsev, M. Understanding and influencing attackers' decisions: implications for security investment strategies. The Fifth Workshop on the Economics of Information Security, Cambridge, England, June 26-28, 2006.

Daneva, M. (2006) Applying Real Options Thinking to Information Security in Networked Organizations. CTIT Technical Report TR-CTIT-06-11. Centre for Telematics and Information Technology, University of Twente, The Netherlands.

Emory Univesity (2007) Why IT Security Can Instil Confidence in a Company's Reputation and Brand. Knowledge @ Emory (http://knowledge.emory.edu/article.cfm?articleid=1075)

Faloutsos, M., Faloutsos, P., and Faloutsos, C. On power-law relationships of the Internet topology. ACM SIGCOMM Computer Communication Review, 29, 4 (1999), 251-262.

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

Gordon, L.A., and Loeb, M.P. (2002b) "Return on Information Security Investments: Myths vs. realities," Strategic Finance, 84(5), 26-31.

Gordon, L.A., Loeb, M. P., Lucyshyn, W., and Richardson, R. (2005) Tenth Annual CSI/FBI Computer Crime and Security Survey. Computer Security Institute.

Hauske, K., (2006) "Returns to Information Security Investment: The Effect of Alternative Information Security Breach Functions on Optima Investment and Sensitivity to Vulnerability," Information Systems Frontier, 8, 338-349.

Huang, C.D., Hu, Q., and Behara, R.S. (2006) “Economics of Information Security Investment in the Case of Simultaneous Attacks,” The Fifth Workshop on the Economics of Information Security, June 26-28, Cambridge, England.
Huang, C.D., Hu, Q., and Behara, R.S. (2008) “Economics of Information Security Investment in the Case of Simultaneous Attacks,” International Journal of Production Economics, 114 (2), 793-804.
Jennex, M.E. and Zyngier, S. (2007) “Security as a Contributor to Knowledge Management Success,” Information Systems Frontier, 9, 493-504.
Jonsson, E. and Olovsson, T. (1997) “A Quantitative Model of the Security Intrusion Process Based on Attacker Behavior,” IEEE Transactions on Software Engineering, 23(4), 235-245.
Kumar, R., Raghavan, P., Rajagopalan, S., Sivakumar, D., Tomkins, A., and Upfal, E. The web as a graph. Proceedings of the Nineteenth ACM Symposium on Principles of Database Systems, Dallas, Texas, May 15-17, 2000, 1-10.
Martin, L. (2006) “The Statistical Value of Information,” Workshop on the Economics of Securing the Information Infrastructure, October 23-24, Washington, D.C.
Mercuri, R. T. (2003) “Analyzing Security Costs,” Communications of the ACM, 46(6), 15-18.
Pastor-Satorras, R., and Vespignani, A. Epidemic spreading in scale-free networks. Physical Review Letters, 86, 14 (2001), 3200-3203.
Schechter, S.E. Toward econometric models of the security risk from remote attacks. IEEE Security & Privacy, 3, 1 (2005), 40-44.
Wang, J. (2004) How May IT Security Affect Competitive Advantage?” The Fourth ABIT Annual Meeting, Monroeville, Pennsylvania.
Watts, D.J., and Strogatz, S.H. Collective dynamics of “small-world” networks. Nature, 393 (1998), 440-442.