Association for Information Systems
AIS Electronic Library (AISeL)

ECIS 2007 Proceedings

European Conference on Information Systems (ECIS)

2007

A System Dynamics Model of Information Security Investments

Ravi Behara
Florida Atlantic Universit, rbehara@fau.edu

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

Qing Hu
Florida Atlantic University, qhu@fau.edu

A SYSTEM DYNAMICS MODEL OF INFORMATION SECURITY INVESTMENTS

Behara, Ravi, Florida Atlantic University, 777 Glades Road, Boca Raton, FL 33431, USA, rbehara@fau.edu

Huang, C. Derrick, Florida Atlantic University, 777 Glades Road, Boca Raton, FL 33431, USA, dhuang@fau.edu

Hu, Qing, Florida Atlantic University, 777 Glades Road, Boca Raton, FL 33431, USA, qhu@fau.edu

Abstract

Information security management has become an increasingly serious and high-stake challenge to organizations, due to growing reliance on the Internet as the business platform, the intrinsic vulnerability of Internet technologies, and the increasing value of information stored in information systems. Because of the complex nature and the large number of closely coupled variables associated with information security problems, sophisticated analytical tools are needed to help decision makers to address the management of information security with limited resources. In this paper, we adopt the system dynamics approach to security analysis, with the help of an information security life cycle model. By identifying the causal loop among such variables as the attractiveness of information target and the total number of attacks, we develop a system dynamics model for analyzing the effect of organizational security investments in the attack stage of the information security life cycle. Using this model, we simulate a number of security management scenarios and demonstrate the feasibility and validity of the system dynamics approach. The model presented in this paper is adaptive, and its parameters and relationships can be calibrated with empirical data for further refinement and customization for specific situations in real world organizations.

Keywords: information security, system dynamics, simulation, security investment, security management, security modelling.

1. INTRODUCTION

Information security incidents have become routine occurrences in recent years. In the ten year period from 1993 to 2003, the number of security incidents reported to CERT increased from 1,334 to 137,529 per year (CERT, 2006). Although most of the earlier attacks were largely for bragging rights of the hackers with benign consequences, recent security attacks were often aimed at stealing valuable information, such as customer credit card numbers and bank account information, for monetary gains, identity theft, and other criminal intents. These attacks have resulted in financial losses amounting to hundreds of millions of dollars to U.S. companies and other organizations including government agencies (Gordon et al., 2004), and possibly in the trillions worldwide (Mercuri, 2003; Cavusoglu et al., 2004).

In response to the increasingly frequent attacks and growing financial and legal risks associated with security breaches, organizations are investing billions of dollars 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. According to a recent CSI/FBI survey, organizations spent between $141 and $643 per employee annually on security-related operating expenses and capital expenditures, and about half of the respondents reporting that one to five percent of their total IT budget is allocated to information security, with some organizations as high as 10% (Gordon et al. 2005). 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, a firm needs to determine the most effective level of information security investment, based on the nature of the information sets it intends to protect, the configurations of its information systems, the potential loss if a security breach does occur, and the attack environment that it faces. Recent academic research in the economics of information security, albeit limited, intends to address this issue (e.g., Gordon et al., 2002; Cavusoglu et al. 2004, Huang et al, 2005, 2006).

In this study, we submit that the information security is a complex system of many closely and circularly coupled variables, and seek to examine the issue of determining the most effective ways of managing security investment based on the principles of system thinking and the methodology of system dynamics (Sterman, 2000). What sets this approach apart from traditional analytical methodologies is that it considers a large number of identified factors pertaining to information security systemically and their interactions dynamically, instead of assuming that the relationships are sequential (as in the case of game theory), deterministic (as in financial analysis), or static (as in economic analysis), and often overly simplified (small number of variables). In adopting this approach, we can model the real-world processes with dynamic structure that simulates the realistic state of variables and their complex interactions. We believe that the system dynamics approach is particularly salient to the study of information security in organizational settings and can complement studies that are completely quantitative (e.g., economic and game theory analysis) or completely qualitative (socio-technical and organizational analysis).

This paper is arranged as follows. In Section 2, we review the literature on information security investment and point out the gaps that can be filled by a system dynamics approach. And we discuss in detail the foundation of system dynamics, and propose an information security life cycle model as the basis for system dynamics modeling. We then focus on the first stages of the information security life cycle, namely the attack stage, and develop a system dynamics model to examine the various types of investments the firm can make to reduce the number of attacks. Simulation results of this model are presented in the second half of Section 3. Finally, in section 4, we discuss the results, limitations, and future direction of the system dynamics approach.

2. RESEARCH BACKGROUND

2.1 Information Security Investment

When millions of dollars are spent each year by firms for information security related products and services, a natural question top management would ask is: are we over or under spending on information security? Research on the economics of information security investment attempts to shed some lights on this question. Although an important topic academically and in practice, it is still in its early stage. However, significant progress has been made in recent years along three independent research streams. In the first stream, scholars aim to develop more practical methodologies for analyzing the appropriate level of and return on information security investment. These methods, including cost-benefit analysis (Gordon and Loeb, 2006), net present value (NPV) and internal rate of return (IRR) (Gordon and Loeb, 2002b), risk management (Hoo, 2000), bypass rate of security technologies (Arora et al., 2004), and analytic

hierarchical process (AHP) (Bodin et al., 2005), focus on the financial or managerial evaluation of security investments. The second stream is primarily based on classic economic analysis. Scholars adopted utility maximization principle to derive optimal investment level of a firm under a limited number of constraining conditions (Gordon and Loeb, 2002a; Huang et al., 2005, 2006). However, both of these approaches treat information security as a static process with deterministic outcomes, which is usually not the case in the real world. In the third research stream, scholars use game theory to analyze the interactions between the attackers and defenders of information security (Cavusoglu et al., 2004, 2006).

Although these streams of research have yielded some interesting and important results in the evaluation and optimization of security investments, they all are based on the assumption that equilibrium can be reached, among the few factors that they choose to analyze, in abstract information security scenarios. In reality, however, information security is a complex system with such variables as attacker intention, firm's defense, recovery processes, security policies, operating procedures, human behavioural factors, property and value of information sources, and intrinsic vulnerability of systems, to name just a few. The relationships of these variables are nonlinear, closely coupled, and often circular. And any change in one can have significant and hard-to-predict impact on others. In addition, it is difficult, if not impossible, to identify the all important dependent variable(s) that traditional analytic approaches aim to optimize. It is this complex nature that motivates us to adopt a systemic approach, namely the system dynamics, for examining the issues related to information system security and the impact of security investments.

2.2 The System Dynamics Approach

The system dynamics techniques were developed in the 1950s by Forrester and his colleagues at MIT, originally intended to model managerial and industrial processes based on control principles (Forrester, 1961, 1968). The main focus of the system dynamics approach is to employ circular causality and feedback structure to simulate observed behavior of complex systems. As a discipline, system dynamics is grounded in the theory of nonlinear dynamics and control developed in mathematics, physics, and engineering (Amaral and Ottino, 2004; Sterman, 2000). Mathematically, the basic structure of a system dynamics model is a set of linear or non-linear, coupled, first-order differentiation equations in the following form:

$$\frac{dx_n}{dt} = f(x_n(t), u(t)), \tag{1}$$

and

$$x_n(t) = g(x_n^1(t), ..., x_n^k(t)), \tag{2}$$

where $x_n(t)$ is a variable in the system structure, $u(t)$ is the vector of exogenous input, $x_n^i(t)$, i = 1...k, are other variables in the system structure that are coupled with $x_n(t)$, and $f(\ )$ and $g(\ )$ are two (likely nonlinear) functional forms. Note that with the circular feedback nature of system dynamics, there is no clear delineation of dependent and independent variables in the set of differential equations (1) and (2). That is, $x_n(t)$ is likely to be an argument of the expression (2) for another variable, say, $x_m(t)$. Instead, variables can be either endogenous or exogenous to the model's structure, or controllable or uncontrollable from the firm's perspective.

To adopt system dynamics approach to analyze managerial or organizational problems involves three steps:

- Creating a model to represent the real-world structure. According to Forrester, system dynamics models are formulated to unite "the structure of the real system, the behavior of the real system, the model, the behavior of the model, and the model builder's purpose" (Forrester, 1979, p.15). Such dynamic structure serves as hypotheses that characterize the interdependency, interaction, feedback, and causality of endogenous factors within the systems being studied (Matinez-Moyano, 2003).
- Establishing the functional relationships among the variables in the dynamic structure, as represented by equation (2), and the "dynamics" of the variables, represented by equation (1). These relationships can be analytical, empirical, or numerical in nature.
- From a set of initial values, iterating (1) and (2) for all variables simultaneously to either reach a steady state or for a set period of time. This is done often with the aid of computer simulation programs.

The results of the computer simulation (Step 3) will give a dynamic picture of the behaviour of the system under study. However, a rigorous and stable model (Step 1) and the variable relationships therein (Step 2) are crucial to the usefulness of the system dynamics approach, because "the most important and difficult step in system dynamics is perception of a model structure appropriate to the chosen purpose" (Forrester, 1979, p. 14). Although "trial and error" is often used to improve the modeling, techniques such as boundary scenarios and sensitivity analysis can be employed to ensure the stability and robustness of the system dynamics models. Other internal and external verification and validation methods are often necessary to make certain the model's functional integrity, structural integrity, completeness, and relevance.

Scholars in the information systems discipline have just started using the principles and techniques of system dynamics in analyzing a variety of IT-related issues with complex structure and relationships. King and Burgess (2006) examine the dynamics of ERP implementation success by modeling the influences of critical success factors identified in prior research literature, in the hope that better understanding of the implementation dynamics would lead to better implementation strategies. In a similar fashion, Marqueza and Blanchar (2006) use a system dynamics model to simulate the impact of investments in product design and marketing on the revenue growth and profitability, taking into account factors such as consumer behavior and competitors responses. They also demonstrate how such a simulation model can be used as a decision support system for corporate planners to evaluate spending trade-offs in product features, services, support, integration, channel incentive, pricing, and advertising.

In this paper, we submit that the system dynamics approach is particularly salient for the analysis of information security. Previous research has used system dynamics to model areas of information security such as insider threats (Anderson et al., 2004; Melara et al., 2003; Rich et al., 2005), human factors in risk-dependent compliance (Gonzalez and Sawicka, 2002), and the dynamic interaction of threats and counter-measures (Saunders, 2003). Our focus is on the effect of information security investments and, with the help of the Information Security Life Cycle model discussed below, how system dynamics models and their computer simulations help determine the optimal allocation of such investments.

2.3 Information Security Life Cycle Model

Many studies of information security investments are based on a single-stage model, where the security events take place in the transition of two states. For instance, the Gordon and Loeb model (2002) assumes that a breach converts security attacks to losses, and the firm in question invests to prevent such breaches from happening. This single-stage assumption simplifies modeling efforts in general, but inevitably restricts a model's ability to simulate real-world

situation. In reality, firms have multiple levels of security defense in which to invest, and each level has different impact on the ultimate outcome of security events.

In this study, we extend the multi-stage risk assessment methodology by Drake and Morse (1997) and propose an Information Security Life Cycle (ISLC) model for the analysis of security investment. In the ISLC model, a security event can traverse through four stages over time (see Figure 1):

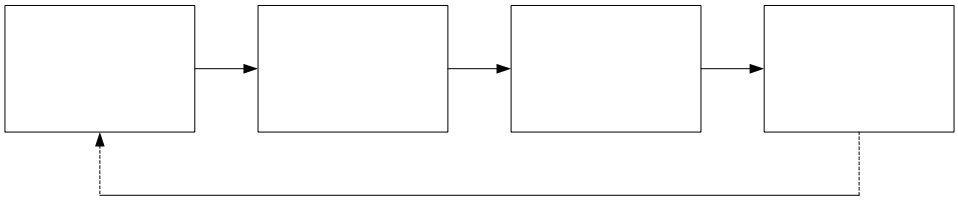

Figure 1. Information Security Life Cycle Model

- Attack, issued by an adversary, reaches the firm's information systems;
- Breach happens when an attack compromises and penetrates the information systems;
- Loss results from those security breaches that are not negated by the firm's security measures; and
- Recovery happens when the loss is limited, and the firm returns to the first stage of fielding attacks.

We believe that ISLC is well suited for using with the system dynamics approach for the following reasons. First, each stage represents a well-defined sub-system that can be modeled separately with a set of endogenous variables. In addition, the system dynamics models of the adjacent stages can be linked through a limited set of variables, reducing the complexity of modelling the whole system of information security. Lastly, investment classes identified in each stage can be used as the basis for investment allocation within the models. In the next section, we develop a system dynamics model for the first stage, the Attack stage, as a demonstration and also validation of system dynamics approach to information security research.

3. SYSTEM DYNAMICS MODEL

3.1 Model Development

Figure 2 shows our system dynamics model for the Attack stage in the ISLC, the result of a combination of literature review and rounds of discussions among the co-authors. The core structure (or the main causal loop) of the model is based on the dynamic interactions between the actions of the attackers and the target firm, influencing and influenced by such factors as perceived costs, perceived benefits, and perceived ease of attack (Cremonini and Nizovtsev, 2006; Jonsson and Olovsson, 1997; Leeson and Coyne, 2006; Liu, Zang, and Yu, 2005).

Typically, causal loops in system dynamics model come in two types: a reinforcing loop, where the variables involved reinforce one another, and a balancing loop, where the variables interact with one another in an oscillatory behavior. We argue that the main causal loop in the Attack phase is largely one of reinforcement; that is, the successes of attacks lead to more attacks, and

reduced attack frequency leads to still fewer attacks. Although such attack dynamics is plausible, the implied result of zero or infinite number of attacks from this reinforcement is unrealistic. Constraining such a reinforcing loop are firm's investments in information security and the effectiveness of such investments. The likely outcome of these constraints is a balancing behavior among the firm's managers and the attackers.

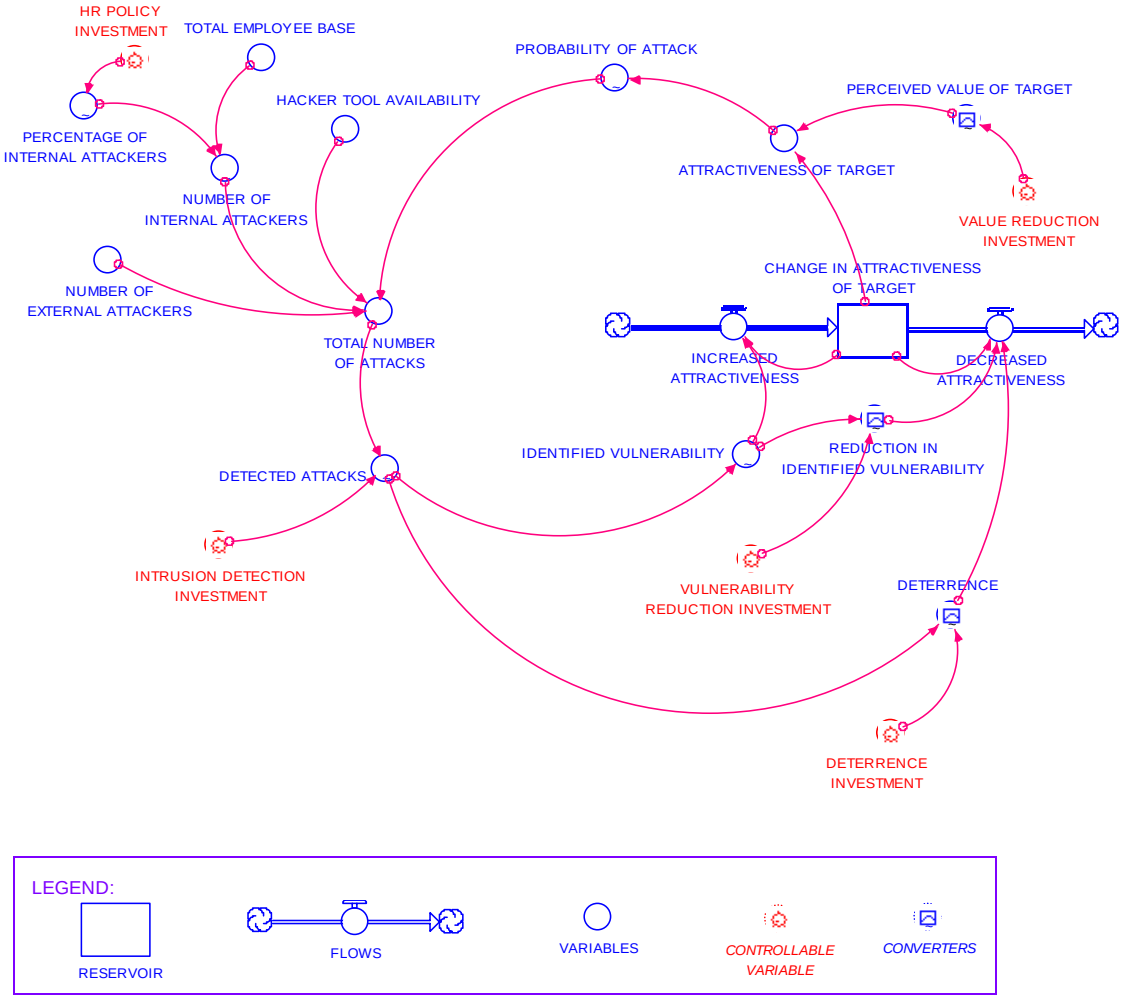

Figure 2. System Dynamics Model of the Attack Stage

As constraints to the reinforcing loop, information security investments seek to increase the costs of attack, reduce the benefits of attack, and add to the difficulty of attack. In our model, investments in this stage take several forms: human resources policy (to discourage internal attackers), detection technologies, attack deterrence technologies and procedures, vulnerability reduction, and information value reduction. The last category includes such actions as parsing corporate data into small clusters, removing sensitive information from vulnerable servers, and segmenting objects using neutral indexes, all aimed to reduce the value of information and information systems to potential attackers. The other investment categories should be self-explanatory. These investments are the controllable variables in the model; all other variables are either directly or indirectly influenced by them. The uncontrollable variable that is of particular

interest is the total number of attacks on the information system of the target firm, which is expected to be reduced to the extent possible with the above investments.

The embedded logic of the model in Figure 2 is as follows. The total number of attacks predicates on the total number of attackers—internal and external—and the availability of hacking tools, which increases the productivity of attackers. The number of external attackers is an exogenous, uncontrollable variable, while the number of internal attackers is represented as a percentage of the total number of employees in the firm and can be reduced by the investments in human resource policies that the firms undertakes to minimize the incentive for attacks from within. The number of attacks is also a function of the probability that a potential attacker would actually attack. This attack probability is a feedback variable from the reinforcing causal loop.

Attacks are known to the firm only when they are detected, and the extent of detection increases with the investment in intrusion detection technologies. The detection of attacks has two effects. As the number of detected attacks increases, the number of identified vulnerabilities also increases (although not in a proportional manner, because a single vulnerability is likely to attract multiple attacks). The more identified vulnerabilities there are, the more attractive the firm's information systems are to the attackers, and the more incentive for the firm to invest in reducing the vulnerability. On the other hand, the need for deterrence increases with the number of detected attacks, and the investment in deterrence would reduce the attractiveness of the target. In summary, while the attractiveness of the target increases with identified vulnerabilities (the reinforcement), it is diminished by investments that reduce vulnerability and increase deterrence (the constraints).

The attractiveness of the information target is also influenced by the perceived value of the target, which can be reduced with appropriate investments (e.g., not storing customer credit card information on servers but relying on financial institutions to validate and processing credit charges). The probability of attacks is a function of the attractiveness of the information target to the attacker. The model closes and completes the causal loop by connecting the attack probability as a functional argument of the total number of attacks.

3.2 Model Simulation

We use the iThink simulation software package as the tool for simulating the system dynamics model in Figure 2. All of the relationships among the variables as described above were operationalized as empirical functions. Except for the actual number of attacks and number of employees and attackers, all other variables in the model are normalized between 0 and 1.

Simulation models need to undergo verification and validation before being used to generate any useful results. Verification is conducted to ensure the logical structure and internal consistency of the model. Validation ensures the applicability of the model and is usually done through historical data when such data exists, boundary condition testing, or spot checking by managers. At the current stage of this research, we perform preliminary verification and validation of the model by examining the logical flow of the variable relationships, by sensitivity analysis, and by boundary conditions testing.

In what follows we present the simulation results of a few scenarios. The purpose is both to test the validity of the model and to demonstrate typical runs of such simulations.

3.2.1 Scenario A: Equal Investments.

In this base scenario, all investments in the Attack stage are equally weighted. That is, the allocations for intrusion detection investment, HR policy investment, deterrence investment, value reduction investment, and vulnerability reduction investment are all equal and set at 0.2 for

a total of 1. The result of this simulation is shown in Figure 3. We can see that the total number of attacks drops off exponentially as the impact of the investments is felt over time. This demonstrates the effect of the investments as constraints to reinforcing loop of the attack dynamics. It should be noted that, with the investments, the number of attacks does not drop to zero. The asymptotic minimum (~ 4,000 in this case) can be regarded as the balance between positive feedback of the reinforcing loop and the constraining effect of the investments. This result is generally consistent with observed reality.

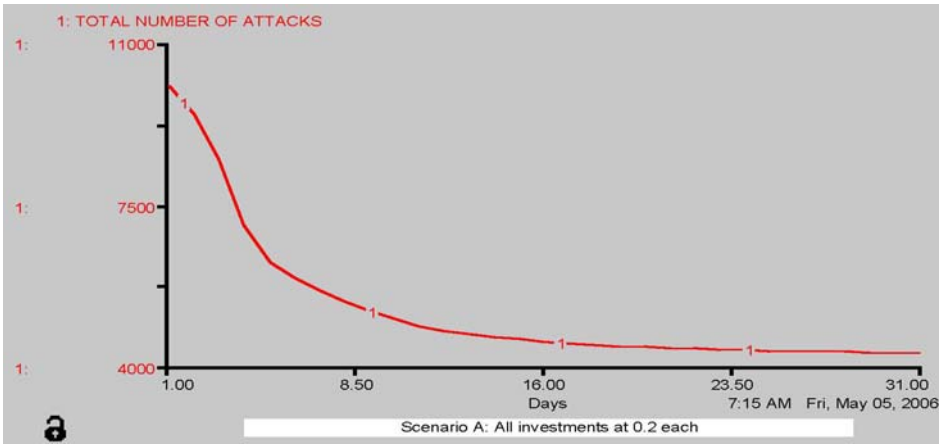

Figure 3.Scenario A: Equally Weighted Investments

3.2.2 Scenario B: Common Investment Practice.

We note that a commonly adopted security management practice is to invest only in intrusion detection and in reducing the identified vulnerabilities. To simulate this common practice, we set these two categories of investment are at 0.5 each, while setting others to 0. The simulation result is presented in Figure 4. We note that, compare to Scenario A in Figure 3, the decay of the number of attacks over time is slower, and the asymptotic minimum is higher. In other words, investments in Scenario B are less effective in reducing the number of attackers than those in Scenario A, and the common practice of security management appears to be inferior to the equal-weight approach.

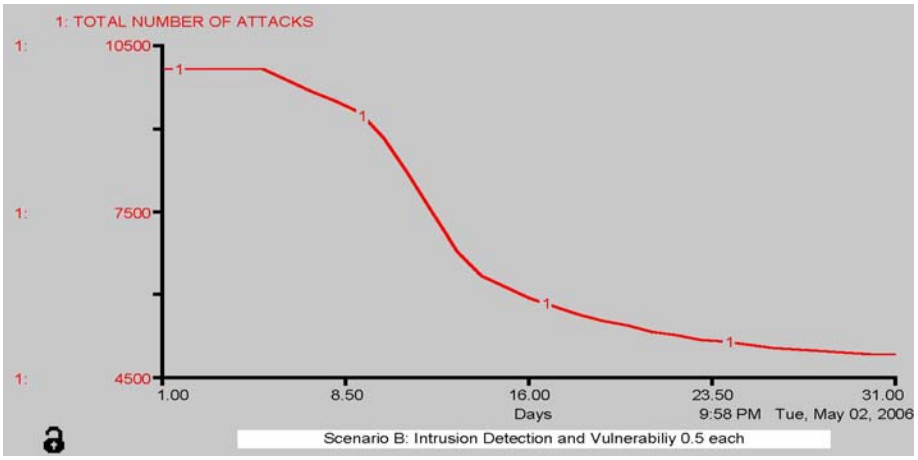

Figure 4.Scenario B: Detection and Vulnerability Reduction Investment

3.2.3 Sensitivity Analysis

We test the stability of the model by applying sensitivity analysis to a select set of variables. First, as shown in Figure 5, we vary the value reduction investment from 0.2 to 1.0 in steps of 0.2, while setting all other investments at 0.2. As expected, the number of attacks drops with increasing investment in this category. But it is important to note that the impact of the initial increase in this investment is significant, while subsequent investment increases generate less and less reduction in number of attacks. This behaviour points to the diminishing return on value reduction investments, a reasonable behaviour of investment.

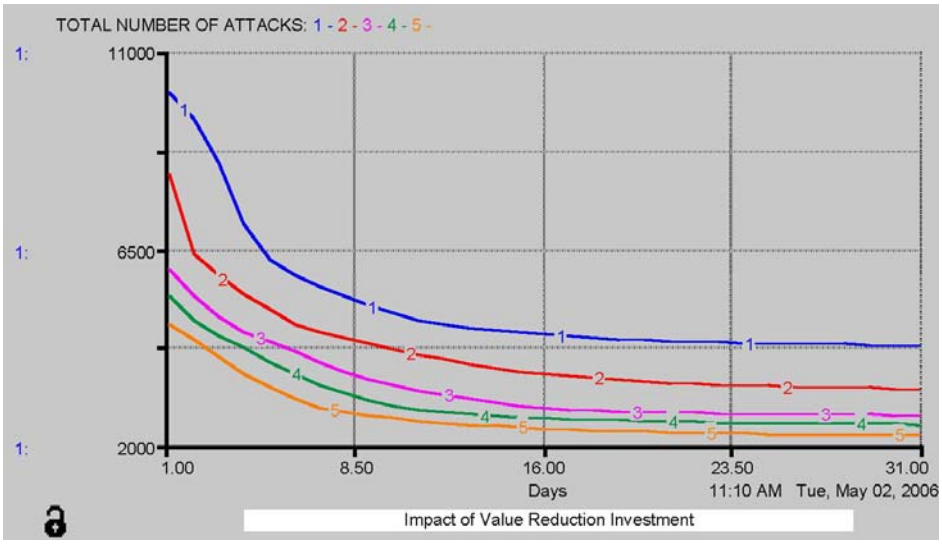

Figure 5. Sensitivity Analysis of Value Reduction Investment

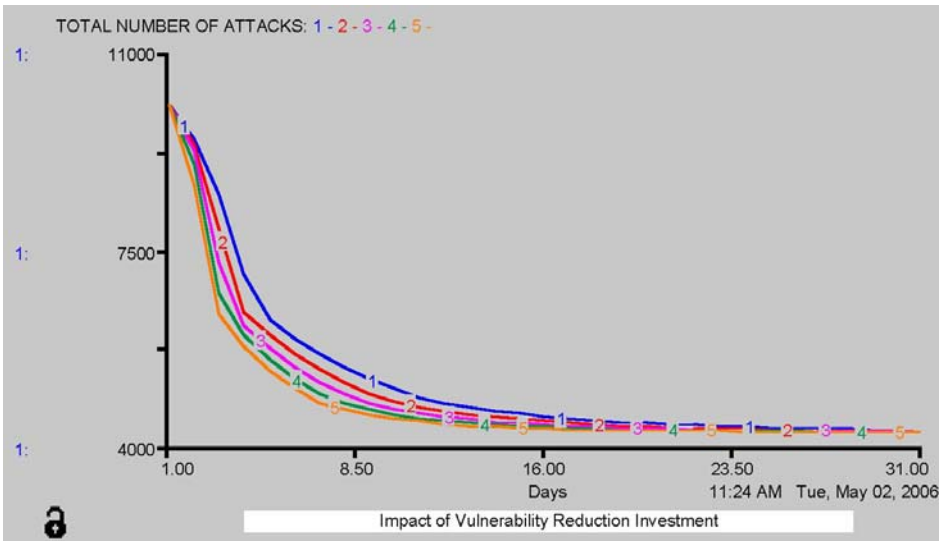

Figure 6. Sensitivity Analysis of Vulnerability Reduction Investment

When similar sensitivity analysis of step-wise increase is applied to vulnerability reduction investments, only the rate of decrease in the number of attacks is affected; the asymptotic minimum remains the same for all investment levels from 0.2 to 1. That is, as shown in Figure 6, larger investment in this category tends to reduce the number of attacks quicker than smaller investment, but to the same final level. This result seems consistent with practice, where, in the long run, all attacks aim at exploiting those vulnerabilities that even large amount of investments may not be able to fix easily.

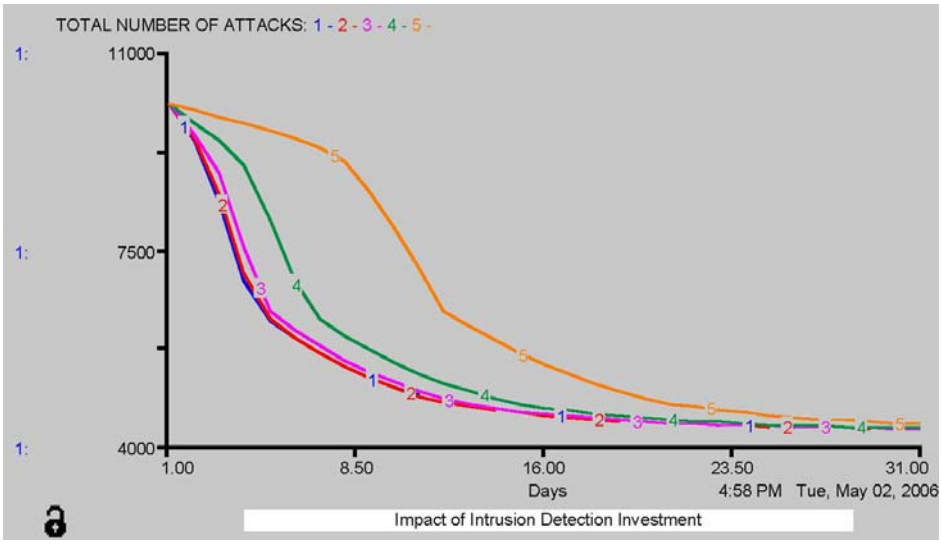

Figure 7. Sensitivity Analysis of Intrusion Detection Investment

Lastly, we test the sensitivity to varying investments in intrusion detection, keeping all other investment levels constant at 0.2. As shown in Figure 7, we find that as the detection investment level increases, larger number of attacks persists initially before diminishing to the same level of asymptotic minimum. This is because, with no additional action taken through other security investments, greater number of attacks detected actually increases the attack probability, due to the nature of the reinforcing loop. This result points to an important property of the information system security, namely that higher level of detection alone does not lead to better security.

Based on the results of the sensitivity analysis, we conclude that the model in Figure 2 is stable and congruent to real-world behavior of the information system security in the Attack stage.

4 CONCLUSIONS

As information systems are increasingly embedded into organizational and social processes, information security cannot be considered as a pure technical challenge, nor does it have clear boundaries between internal organizational processes and external environment. Many of today's security breaches in organizations occurred as results of the interactions between internal and external, technical and social, process and behavioural factors that may or may not within the control of the organizations. To better understand the complexity of information system security and effectively manage and control the associated risks, it is helpful to use tools with the capability of incorporating a large number of closely coupled variables and presenting a coherent and logical structure of the interactions and consequences. In this paper, we attempt to address

this need by using the system dynamics approach to the information security analysis. Based on the Attack stage of the ISLC model, we demonstrate how system dynamics models can be developed and utilized in evaluating and comparing investment options. Our preliminary results, based on a few scenarios, show that the common security approach—concentrating security investments in the highly visibly, technical areas such as intrusion detection and vulnerability reduction—is less effective in reducing the number of attacks than a simplistic approach, where investment dollars are equally divided among all the available security measures. And the sensitivity analysis validates the stability and logical structure of our model.

It is important to note that our model presented in this study serves as a "proof of concept" for the system dynamics approach in the field of information security. Although limited and preliminary, this model already offers interesting practical implications. It is our intention to further develop the model in the future. For example, models for the other three stages of the ISLC need to be developed to provide a complete picture of information security. Another important direction would be to calibrate the parameters and the relationships in the current model with empirical data. And further study to validate the effectiveness of this system dynamics against traditional methodologies in the management of information security investment is also needed.

References

Amaral, L.A.N. and Ottino, J.N. (2004) :Complex Systems and Networks: Challenges and Opportunities for Chemical and Biological Engineers," Chemical Engineering Science, 59, 1653-1666.

Anderson, D.F., Cappelli, D.M., Gonzalez, J.J., Mojtahedzadeh, M., Moore, A.P., Rich, E., Sarriegui, J.M., Shimeall, T.J., Stanton, J.M., Weaver, E., and Zagonel, A. (2004) "Preliminary System Dynamics Maps of the Insider Cyber-Threat Problem," Proceedings of the 22nd International Conference of the System Dynamics Society, Oxford, England, July 25-29. Available online at http://www.cert.org/archive/pdf/InsiderThreatSystemDynamics.pdf. Last accessed on April 29, 2006.

Arora, A., Hall, D., Pinto, C.A., Ramsey, D., and Telang, R. (2004). "Measuring the Risk-Based Value of IT Security Solutions," IT Professional, 6(6), 35-42.

Bodin, L.D., Gordon, L.A., and Loeb, M.P. (2005) "Evaluating Information Security Investments Using Analytical Hierarchy Process," Communications of the ACM, 48(2), 79-83.

Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004) "A Model for Evaluating IT Security Investments," Communications of the ACM, 47(7), 87-92.

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.

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.

Marco, C. and Nizovtsev, D. (2006) "Understanding and Influencing Attackers' Decisions: Implications for Security Investment Strategies," Proceedings of the Fifth Workshop on the Economics of Information Security, June 26-28, Cambridge, England.

Drake, D. and Morse, K. L. (1997) "Applying the Eight-Stage Risk Assessment Methodology to Firewalls," Proceedings of the 13th Annual Computer Security Applications Conference (ACSAC'97), 44-52.

Forrester, J.W. (1961) Industrial Dynamics. Cambridge, MA: MIT Press.

Forrester, J.W. (1968) Principles of Systems. Cambridge, MA: Wright-Allen Press.

Gonzalez, J.J., Sawicka, A. (2002) “A Framework for Human Factors in Information Security,” Proceeding of the WSEAS International Conference on Information Security, Rio de Janeiro, Brazil.
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. (2004) Ninth Annual CSI/FBI Computer Crime and Security Survey. Computer Security Institute.
Gordon, L.A., Loeb, M. P., Lucyshyn, W., and Richardson, R. (2005) Tenth Annual CSI/FBI Computer Crime and Security Survey. Computer Security Institute.
Hoo, K.S. (2000). “How Much Is Enough? A Risk-Management Approach to Computer Security,” Working Paper, Consortium for Research on Information Security and Policy (CRISP), Stanford University, Palo Alto, California,.
Huang, C.D., Hu, Q., and Behara, R.S. (2005) “In Search for Optimal Level of Information Security Investment in Risk-Averse Firms," Proceedings of the Third Annual Security Symposium: Information Security in the Knowledge Economy, Tempe, Arizona, September 8-9, 2005.
Huang, C.D., Hu, Q., and Behara, R.S. (2006) “Economics of Information Security Investment in the Case of Simultaneous Attacks,” Proceedings of the Fifth Workshop on the Economics of Information Security. June 26-28, Cambridge, England.
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.
King, S.F. and Burgess, T.F. (2006) “Beyond Critical Success Factors: A Dynamic Model Of Enterprise System Innovation,” International Journal of Information Management, 26, 59-69.
Liu, P., Zang, W. and Yu, M. (2005) “Incentive-Based Modeling and Inference of Attacker Intent, Objectives, and Strategies,” ACM Transactions on Information and System Security, 8(1), 78-118.
Leeson P.T. and Coyne, C.J. (2006) “The Economics of Computer Hacking,” Journal of Law, Economics and Policy, forthcoming.
Marqueza, A.C. and Blanchar, C. (2006) “A Decision Support System for Evaluating Operations Investments in High-Technology Business,” Decision Support Systems, 41, 472-487.
Martínez-Moyano, I.J. (2003) “Structure as Behavior: Exploring Elements of the System Dynamics Modeling Process,” Proceedings of the 21st International Conference of the System Dynamics Society, New York, New York.
Melara, C., Sarriegui, J.M., Gonzalez, J.J., Sawicka, A., and Cooke, D.L. (2004) “A System Dynamics Model of an Insider Attack on an Information System,“ Proceedings of the 22ndInternational Conference of the System Dynamics Society.
Mercuri, R. T. (2003) “Analyzing Security Costs,” Communications of the ACM, 46(6), 15-18.
Rich, E., Martinez-Moyano, I. J., Conrad, S., Cappelli, D. M., Moore, A. P., Shimeall, T. J., Andersen, D. F., Gonzalez, J. J., Ellison, R. J., Lipson, H. F., Mundie, D. A., Sarriegui, J. M., Sawicka, A., Stewart, T. R., Torres, J. M., Weaver, E. A., & Wiik, J. (2005) “Simulating Insider Cyber-Threat Risks: A Model-Based Case and a Case-Based Model,” Proceedings of the 23rd International Conference of the System Dynamics Society. Boston, MA, July 17-21, 2005. Available online at http://www.systemdynamics.org/conf2005/proceed/index.htm. Last accessed on April 29, 2006.
Sauders, J. (2003) “A Risk Management Methodology for Information Security: The Analytic Hierarchy Process,” available at http://www.johnsaunders.com/papers/risk-ahp/risk-ahp.htm. Last accessed on June 12, 2006,
Sterman, J.D. (2000) Business Dynamics: Systems Thinking and Modeling for a Complex World. New York: Irwin McGraw-Hill.