AMCIS 2012 Proceedings

Proceedings

Information Security Management: A System Dynamics Approach

Derek Nazareth
University of Wisconsin Milwaukee, Milwaukee, WI, United States., derek@uwm.edu

Jae Choi
Computer Information Systems, Alabama State University, Montgomery, AL, United States., jchoi@alasu.edu

Recommended Citation
Derek Nazareth and Jae Choi, "Information Security Management: A System Dynamics Approach" (July 29, 2012). *AMCIS 2012 Proceedings.* Paper 3.
http://aisel.aisnet.org/amcis2012/proceedings/ISSecurity/3

Information Security Management: A System Dynamics Approach

Derek L. Nazareth
University of Wisconsin-Milwaukee
derek@uwm.edu

Jae Choi
Alabama State University
jchoi@alasu.edu

ABSTRACT

Managing security for information assets presents a challenging task. The need for effective information security management assumes greater importance with growing reliance on distributed systems and Internet-accessible systems. Many factors play a role in determining the vulnerability of information assets to security threats. Using a system dynamics approach, this study evaluates information security management strategies from a financial and asset loss perspective, with a view to providing managers guidance for information security decisions.

Keywords

information security, security management, simulation, system dynamics

INTRODUCTION

Recent surveys indicate that information security has become a key issue in the IT industry (Richardson 2011). As security incidents continue to increase in frequency and sophistication (Johnston and Warkentin 2010), it is not surprising that almost all IT trade publications now include a security-related section and several new publications dedicated to IT security have emerged (Cremonini and Martini 2005). Published statistics indicate almost all organizations have made some preventive efforts in areas of firewalls and antivirus programs, and many larger firms have ongoing projects aimed at protecting their assets from internal and external security threats. However, in a number of cases, increases in information security investment are driven by knee-jerk reactions to new perceived risks rather than by pragmatic cost-benefit analyses of solutions (Cremonini and Martini 2005). In addition, many cost-benefit analysis models do not factor in qualitative or nonfinancial criteria, which remain a significant aspect of information security (Bodin et al. 2005).

One of the more pressing issues that security managers face is the selection of appropriate security management strategies. Given the wide variety of security threats that need to be countered, managers need to consider a portfolio of counter strategies, each with different costs and potential benefits. The business value derived by an organization from investment in information security is determined by multiple factors, including security expenditure, the magnitude of any damage sustained and averted, the loss of reputation, perceived attractiveness for follow-up targets, among others. It has been suggested that the business value associated with security investment is coupled with the preferred level of security which varies depending upon a variety of internal and external factors.

The inability to effectively assess the consequences of decisions about information security investments in an a-priori manner leaves security managers to speculate if the decisions made were the appropriate ones. A model that captures the complexities of the security decision while permitting a systematic exploration of alternative security options would serve as an invaluable aid to security managers. Using the design science research methodology (Hevner et al. 2004), this paper develops a dynamic model that allows security managers to examine the effects of alternative security decisions on the organization's information assets. The model can be adapted and calibrated for different organization contexts.

The rest of the paper is organized as follows. The theoretical background that serves as the foundation for building the model of information security management is presented in the next section. A dynamic model of the mechanics underlying the impact of security attacks and their financial implications is assembled and presented thereafter. The model is used to examine the implications of alternative security investment strategies. Research and managerial implications of the simulations round out the paper.

THEORETICAL BACKGROUND

Security in the information systems area has been a topic of interest for a while, with studies dating back to the early nineties (Straub 1990, Baskerville 1993). A number of aspects of security have been studied, including external attacks, internal abuse, password security, among others. Despite the importance of the topic, there are comparatively few published studies. Some of this may reflect the reluctance of organizations to reveal information about their security procedures, and hence elect to not participate in security studies (Kotulic & Clark 2004). Even the latest CSI study, which surveys security personnel, has indicated a drop in the number of responses and the response rate when compared to prior studies (Richardson 2011). With the greater urgency associated with effective security, mainstream journals have devoted special issues to it, and a host of security oriented journals have emerged. A number of meta-analyses of research in information security have emerged (Baskerville 1993, Dhillon and Backhouse 2011, Siponen 2005, Sunyaev et. al. 2009), calling for a more holistic approach to addressing information security issues. They identify areas needed additional research, including the economics of information security. Though economists have studied the interplay between economics and security for a considerable period, it is only recently that research on the economic aspects of information system security has gained more attention. One stream of research is devoted to economic modeling of security investments using a net present value approach, examining optimal expenditure levels (Gordon and Loeb 2006), risk management (Hoo 2000), and bypass rate of security technologies (Arora et al. 2004). A different stream uses classic economic analysis, adopting the utility maximization principle to derive optimal investment levels of a firm under a limited number of constraining conditions (Gordon and Loeb 2002b, Huang et al. 2005). Yet other approaches utilize the principle of equating marginal financial benefits of information security to the marginal financial costs of such security (Gordon and Loeb 2002a).

These research efforts typically adopt a quantitative approach to the security problem. However, a major aspect of security relates to qualitative and non-functional criteria. In an effort to include these, some researchers have employed the analytic hierarchy process (AHP) to combine quantitative and qualitative criteria (Bodin and Epstein 1999, Bodin and Gass 2003). These studies typically adopt a static view of the information security problem. In actuality, information security is a complex system of many closely and circularly coupled variables. It involves people, organizational factors, technology, tasks, and the working environment (Carayon and Kraemer 2002, Smith and Carayon-Sainfort 1999). In addition, the security management system often involves multiple controls, including technical controls, formal controls, and informal controls (Dhillon 2001). Technical controls refer to mechanisms that protect the system from incidents or attacks. Formal controls represent business structures and processes that ensure the correct general conduct of business and reduce the probability of an incident or an attack. Informal controls address the culture, value and belief system of the organization.

Clearly, information system security is not just a matter of implementing technical security mechanisms (Melara et al. 2003). Diverse factors and dynamic relationships among them need to be investigated. The dynamic aspects of information security can be captured through simulation studies. Several simulations options are available for understanding the dynamic aspects of information security, including discrete event simulation, continuous simulation, system dynamics, and agent-based simulation, among others. Discrete event simulation models the phenomenon at the individual transaction level, in this case at the level of individual attacks, and provides security managers with the ability to examine the efficacy of different security strategies under a variety of attacks within a specified period. Continuous simulation deals with dynamic systems that are amenable to description via differential equations, and is less applicable as a viable technique given the discrete nature of security attacks. Agent-based simulations are useful in contexts of independent decision-making entities that cooperate to accomplish an overall objective. System dynamics uses a combination of first order linear and non-linear difference equations to relate qualitative and quantitative factors within and across time periods (Sterman 2000) and is based on principles developed by Forrester to study managerial and dynamic decisions using control principles (Forrester 1961).

System dynamics has been employed by some researchers to investigate information security. Behara et al. (2007) developed an information security life cycle model, incorporating four stages to investigate security attacks. Their study primarily investigates the impact of investment in HR policy, intrusion detection, vulnerability reduction, value reduction, and deterrence on the overall number of attacks experienced. Their findings indicate that investment in all areas tends to be more effective than traditional investment strategies that focus on high profile areas only. Another study (Melara et al. 2003) utilized system dynamics to develop a model for insider attacks, focusing on the 1996 Omega case addressing technical security controls, workplace discontent, motivation, and time-bomb attacks. Other efforts in information security using system dynamics focus on insider and outsider threats by modeling detection ability, motivation for attacks, trust, and deterrence (Gonzalez and Sarriegui 2004).

This research uses system dynamics to investigate the effect of different security decisions on an organization's information assets. System dynamics was chosen for the simulation as it permits examination of relationships between constructs within a time period, as well as across time periods. It describes a model that examines security policies, vulnerabilities, attacks, relating them to security costs and overall damage sustained. It provides managers with the ability to investigate the effect of putting resources into alternative security channels and their impact under a variety of different conditions. While the model cannot cover all security attacks and scenarios, and given that a completely impregnable system is infeasible, it does provide managers with insights into the relative risk tradeoffs under different scenarios. This research adopts a design science methodology using the system dynamics model as the artifact of interest. Demonstration of the utility of the artifact is accomplished through successful execution of the model under a variety of conditions. Managerial and research implications of the study are discussed.

INFORMATION SECURITY MANAGEMENT MODEL

Information security effort and resources can be deployed in a number of areas including policy formation, planning, risk analysis, prevention, deterrence, detection, mitigation, investigation, damage analysis, recovery, and compliance, among others. While there have been several attempts to characterize information security activities using a life-cycle framework, the constant need for security, coupled with an evolving and continually expanding set of threats, makes it more of an evolutionary process involving many activities within a ceaseless timeframe. The model for information security management is driven by security attacks on information assets, and addresses efforts to reduce the attacks, as well as efforts to recover from the attacks and make the assets more secure. It draws from areas of software risk assessment, software vulnerability, attack motivation, threat detection, deterrence, and security costing. It was developed over several rounds of iteration and testing, and is depicted in Figure 1. We provide a quick overview of the notation. Items in rectangles represent stocks that can accumulate or deplete over time. Stocks are affected by flows, which are represented by a double arrow and valve symbol. Flows draw from or empty into infinite reservoirs. Other variables on the diagram represent converters, which have values that are specified for the given time period. Values of converters are determined by other converters through connectors. Connectors are signed to indicate if an increase in one will lead to an increase in another. The signs characterize the loops in the model. Loops can be reinforcing (all positive signs), or balancing (at least one negative sign). Reinforcing loops, if unchecked, will eventually lead to zero or infinite values for the converters involved. Balancing loops will lead to oscillatory behavior, and possibly equilibrium.

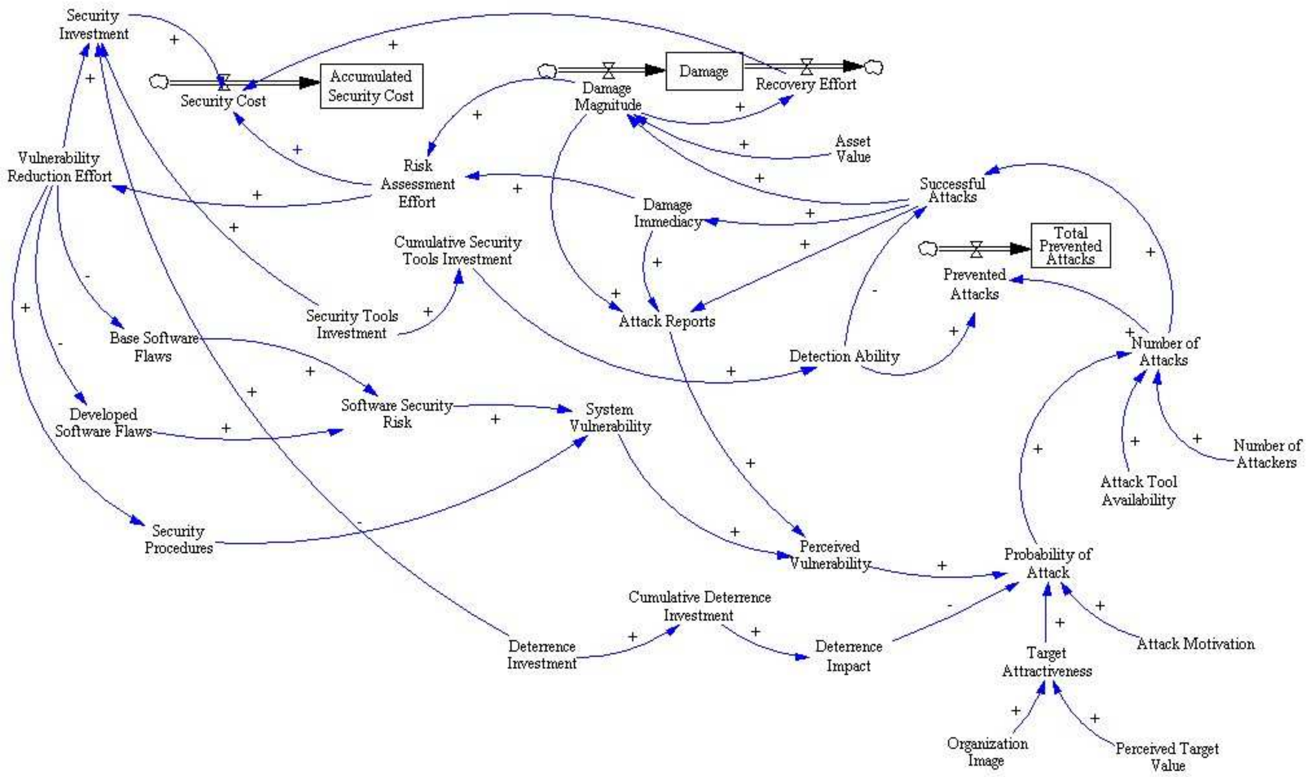

Figure 1. Information Security Management Model

The segment on security attacks is described first. The organization's image, coupled with the perceived target value shape the target attractiveness. The attractiveness, in conjunction with the attacker's motivation, the perceived vulnerability of the organization's information assets, and the deterrence mechanisms in place will influence the probability of attack. This, coupled with the number of attackers (both internal and external), and the availability of tools to launch the attack determine the number of attacks the organization faces. At this point, the model does not differentiate between attacks on different information assets. Clearly, there will be differential attacks on different assets. This model looks at the aggregate picture, and does not concentrate on individual attacks. In a similar vein, it does not parse the attacks into different types, e.g. denial of service, hacking, phishing, keystroke capture, virus attacks, SQL injection, etc. It is expected that a majority of the attacks will be detected by existing security tools, e.g. firewalls, intrusion detection systems, anti-virus programs, malware detection programs, among others. These are characterized as prevented attacks. The balance represent successful attacks. Successful attacks will be manifest in various ways and have considerably different impacts. Some of them will cause little damage, while others will have a more pronounced impact. The damage caused by successful attacks is captured on two dimensions, the magnitude of the damage, as well as the urgency needed to act to recover from the damage, termed damage immediacy in the model. Successful attacks will also create some publicity, captured as attack reports in the model. Attack reports are manifest in a number of ways, including site unavailability, organization acknowledgements of attacks, claims made by the attackers, and reports filed with governmental agencies for compliance purposes. The damage magnitude, damage immediacy, and the number of successful attacks, shape the extent of attack reports. Publicized attack reports will determine the perceived vulnerability of the organization's information assets, thus completing the attack loop. This is a reinforcing loop, indicating that successful breaches will lead to more attacks, and effective prevention of attacks will cause attackers to look to other targets. In an extreme scenario, a reinforcing loop either drives the values to zero or infinity. However, if the model is constructed in a rigorous manner, this behavior is not likely to be manifest.

Another segment of the model deals with risk and recovery, and also relates to system vulnerabilities. Any damage sustained through a successful attack will initiate a recovery effort. Depending on the damage, the extent of recovery effort may be simple to complex, and may involve a trivial to a substantial amount of time. Recovery could be as simple as restoring data from a backup, or may involve rebuilding several servers, including software and hardware reconstruction. The damage magnitude will also trigger a fresh risk assessment effort – mostly likely not an entire reassessment, but an incremental one. An assessment of outstanding risk triggers activity to reduce existing vulnerabilities. These could involve changes to access and security procedures, or changes to the software to reduce vulnerabilities. Software vulnerabilities could be present in the infrastructure software including the operating system, operating environment, or the tools used to assemble software. Often these take the form of known bugs and trapdoors, and can be easily fixed. Vulnerabilities could also be present in the code that is written in-house, often manifest as lax security, lack of appropriate encryption, no checks for security bypass attempts, among others. As indicated in the model, these are inversely related to the vulnerability reduction effort, indicating that they are expected to drop with increased vulnerability reduction effort. The vulnerabilities and the strength of the security procedures will determine the overall system vulnerability, which feeds the perceived vulnerability, thereby completing a different loop. This is a balancing loop, and will compensate for the reinforcing loop on attacks.

The final segment of the model relates to security investment and costs. Organizations invest in deterrent actions as well as security tools to detect and prevent attacks, and these represent the input costs in this case. These investments typically accumulate, though not in strictly linear fashion. The cumulative security tools investment determines the ability to detect attacks. In a similar vein, the cumulative deterrence investment shapes the deterrence impact, which forms part of the attack loop. With the vulnerability reduction effort, these investments constitute the security investment for the organization. The security cost includes this investment, and the costs incurred due to recovery and risk assessment efforts.

SIMULATION RESULTS

The simulation was conducted using Vensim® PLE, a fully functional system dynamics software package from Ventana Systems, Inc. It was run over a period of 30 months, representing a medium term security planning horizon. While it is tempting to simulate for longer terms, the uncertainty of environmental conditions over an extended period precludes making meaningful assessments and predictions. The experiments are conducted with two objectives – to validate that the model is performing realistically, and to understand the impact of different security policies and investments on the overall attacks, damages, and security costs.

Base Scenario

The base scenario for the model was calibrated using median values for the dimensionless variables, and a set of plausible options for other variables. This included an asset base of $5,000,000, the number of attackers pegged at 100, and the security tool investment set at $5000 at the start of every year, with deterrence expenses of $2000 every six months. After running the model, the number of attacks, total damages, and overall security costs were tracked. These results appear in Figure 2.

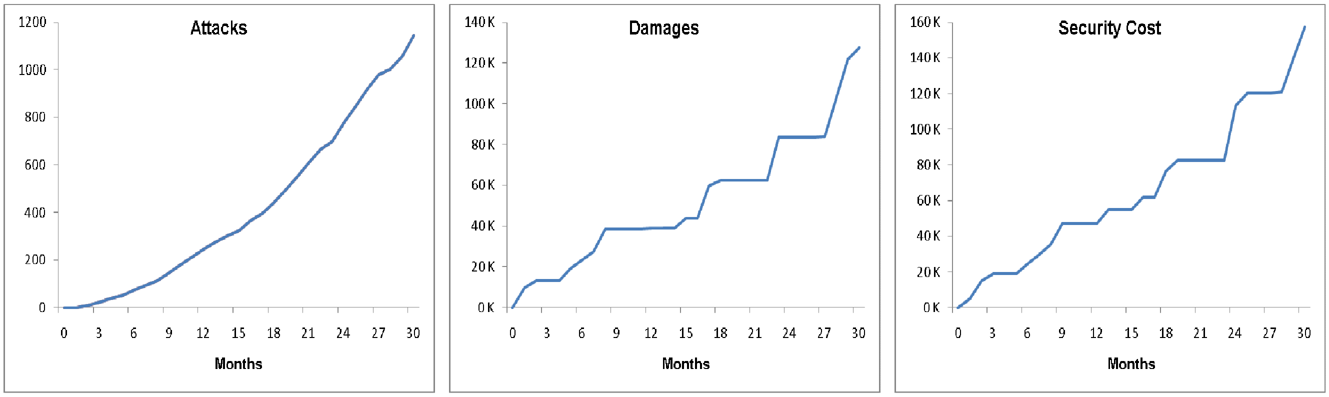

Figure 2. Simulation Results for Base Scenario

Monthly data for the variables tends to be rather spiky in nature, and an aggregation over time provides a better sense of the trends involved. The total number of attacks demonstrates an increasing trend for this organization, though there are periods of lulls in the pattern. Not all attacks are successful, and only some cause damage. Variability in the attack severity leads to variability in the damages incurred. Some disproportionate damages were incurred towards the end of the simulation, leading to a spike in the cumulative security cost. An examination of the other variables in the simulation indicated that they were consistent with expectation. Sensitivity and perturbation analysis was performed by systematic variation of key input parameters. Taken together, these constituted the behavioral validation of the model. In addition, the model was structurally tested using a multiple strategies, including boundary analysis, structural verification, parameter verification, and dimensional consistency.

Alternative Security Investment Scenarios

After establishing that the model was structurally sound, and that its behavior was consistent with expected trends, it was used to investigate the impact of alternative decisions concerning information security management and investment. The base scenario was altered to monitor the effect of different security investments. Separate scenarios were considered for variations in the security tool investment and deterrence investment. These were then compared to the base scenario to obtain a better sense of the impact of alternative security decisions. These results appear in Table 1. All figures represent cumulative values over the duration of the simulation.

Scenario	Attacks	Damages ($)	Security Cost ($)
Base	1,144	127,608	157,556
Low Security Tool Investment	1,393	157,967	217,689
High Security Tool Investment	977	110,592	137,400
Low Deterrence Investment	1,678	143,332	181,867
High Deterrence Investment	926	120,156	150,670

Table 1. Simulation Results for Alternative Security Investments

Some of the results are predictable. As the level of security investment is dropped, the number of attacks experienced increases, as do the damages incurred, as well as the overall security cost. Though not included in this table, recovery costs and vulnerability reduction costs also increase. With increased investment in security, the number of attacks, the magnitude of damage, as well as the overall security costs decrease. However, this trend cannot continue indefinitely, as the increased security investment will offset the reduced damages and recovery effort at some point.

A more telling observation is the relative impact of the security investment. Investment in detection and prevention has a considerably larger impact than investment in deterrence. Detection and prevention reduce the number of successful attacks, which in turn reduce the damages incurred by the organization. Reduced vigilance on this score entails a larger number of successful attacks, and resulting increases in damages, recovery effort, and overall security costs.

Deterrence is primarily aimed at internal attackers, and while the literature suggests that this is sometimes a greater threat than external attackers (Melara et. al. 2003), this is rarely an effective de-motivator for a determined attacker. External attackers are generally not significantly influenced by deterrence practices, since they know that the probability of trace-back is low, and prosecution thereafter is extremely unlikely. These findings have significant implications for security managers, though.

MANAGERIAL AND RESEARCH IMPLICATIONS

The information security management model illustrates that security investments have major implications for the overall costs associated with providing security for information assets. A number of clear implications can be deduced through simulation with the model. The most basic observation is that overall security costs decrease with increased investment in information security. However, this is hardly insightful. An examination of differential investment into different facets of information security yields more telling results.

Investment into tools for detecting and preventing security attacks yielded the greatest payoff. Security tools in this category include anti-virus programs, malware and spyware detection programs, firewalls, intrusion detection systems (network and host versions), SQL injection prevention, among others. Improved detection leads to fewer successful attacks, which in turn entails less damage to the information assets. The implication for security managers is that this area of security investment cannot be overlooked. An organization's information assets are likely to be distributed across many platforms and reside at different locations. The threats and attacks manifest in many ways depending on the mode and site of the attack. A combination of security tools need to be deployed to counter the different forms of attacks, and secure the multiple information assets at multiple locations. The effectiveness of these tools will predictably degrade over time, as newer versions of the attack vectors, as well as newer attack vectors are developed. Security managers need to be constantly vigilant, keeping tools up to date. Several tools, like anti-virus programs, are automatically updated. Other, like firewalls and intrusion detection systems, may need manual updates to block new attack types and sources. While this invariably involves time and effort, the implications are clear. Any attack prevented has definite payoff in terms of reduced damage potential, recovery effort, and subsequent risk assessment and vulnerability reduction effort.

The model suggests that investment in deterrence has a smaller though similar payoff. Deterrence activities take many forms, including setting up policies and procedures to reduce attacks, as well as procedures for dealing with identified attackers. Since these are people-based, they tend to be the weaker links in security. Users often employ easily broken passwords, infrequently change them, and do not protect them sufficiently. Newly installed software is often not adequately secured, as default master accounts may not be appropriately reconfigured. While conventional wisdom suggests that internal attackers are the greater threat in this case, external attacks should not be discounted. Deterrence policies that are set up to deal with internal attackers may not prove adequate. For example, despite threats of discipline and termination for snooping among protected data, coupled with high profile cases involving medical data, employees often engage in these activities. Deterrence has even less restraint or disincentive for external attackers, since they are often not detected, or may be difficult to successfully prosecute. However, even though it will not prevent attacks, investment in security deterrence is necessary.

In terms of overall security investment, while it may be tempting to direct more resources into certain areas given the payoff, it should be borne in mind that investment in security is needed in all areas, since a cutback in one area will essentially set up a new weak link and attacks will be redirected to the new vulnerabilities. This is consistent with prior research that indicates that equal investment in all areas of security led to fewer attacks than differential investment (Behara et. al 2007).

For researchers, this provides a starting point for further exploration of the security investment decisions. A more detailed search of the investment space would form the next logical step. It is expected that in some cases, the added investment in some security areas may offset the benefits, leading to the notion of an optimal investment level. Additional simulations involving changes to other input variables represent further areas for research. These include changes to the number of attackers, their motivation, perceived target value, and the like. A deeper analysis of the process represents yet another area for further exploration. This includes the monitoring of intermediate variables, tracking their behavior under different scenarios, grid mapping of performance, and sensitivity analyses, among others.

CONCLUSIONS

Securing information assets is of critical importance for organizations. Making systems absolutely secure may not be possible, or may be prohibitively expensive. Nonetheless, it is important that some security investments be made, otherwise the organization puts its information assets at significant risk. This research examined the effect of investing in different areas of information security, through the use of a system dynamics model. The model was constructed to include attacks, detection, recovery, risk assessment, and vulnerability reduction. Simulations with the model indicate that investments in security tools designed to detect attacks led to a better payoff than in deterrence activities. However, investments in all areas of security are needed for effectively protecting information assets.

REFERENCES

1. Anderson, R., and Moore, T. (2007) Information security economics - and beyond, in Menezes, A. (Ed.) *Advances in Cryptology 2007*, Springer-Verlag, 68-91.
2. 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.
3. Baskerville, R. (1993) Information systems security design methods: Implications for information systems development, *ACM Computing Surveys*, 25, 4, 375-414.
4. Behara, R., Huang, C. D., and Hu, Q. (2007) A system dynamics model of information security investments, *Proceedings of European Conference on Information Systems, Geneva, Switzerland*, 1572-1583.
5. Bodin, L, and Gass, S. (2003) On teaching the analytic hierarchy process, *Computers and Operations Research*, 30, 10, 1487-1497.
6. Bodin, L. and Epstein, E. (1999) Who's on first – with probability 0.4, *Computers and Operations Research*, 27, 4, 205-215.
7. Bodin, L.D., Gordon, L. A., and Loeb, M.P. (2005) Evaluating information security investments using the analytic hierarchy process, *Communications of the ACM*, 48, 2, 79-83.
8. Carayon, P, and Kraemer, S. (2002) Macroergonomics in WWDU: What about computer and information system security?, *Proceedings of 6th International Scientific Conference on Work With Display Units, Berlin, Germany*, 87-91.
9. Cremonini, M., and Martini, P. (2005) Evaluating information security investments from attackers perspective: the Return-On-Attack (ROA), *4th Workshop on the Economics on Information Security, Harvard University*.
10. Dhillon, G. (2001) Violation of safeguards by trusted personnel and understanding related information security concerns, *Computer and Security*, 20, 2, 165-172.
11. Dhillon, G., & Backhouse, J. (2001) Current directions in IS security research: Towards socio-organizational perspectives, *Information Systems Journal*, 11, 2, 127-153.
12. Forrester, J.W. (1961) *Industrial dynamics*, MIT Press, Cambridge, MA.
13. Gonzalez, J.J., and Sarriegui, J.M. (2004) *System dynamics modeling for information security: An invitational group modeling workshop*, Pittsburgh, PA.
14. Gordon, L. A., and Loeb, M. P. (2006) Budgeting process for information security expenditures, *Communications of the ACM*, 49, 1, 121-125.
15. 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.
16. Gordon, L. A.., and Loeb, M. P. (2002b) Return on information security investments: Myths vs. realities, *Strategic Finance*, 84, 5, 26-31.
17. Hevner, A.R., March, S.T., Park, J., and Ram, S. (2004) Design science in information systems research, *MIS Quarterly*, 28, 1, 75-106.
18. 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
19. 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*.
20. Johnston, A. C., and Warkentin, M. (2010) Fear appeals and information security behaviors: An empirical study, *MIS Quarterly*, 34, 3, 549-566.
21. Kotulic, A.G. and Clark, J.G. (2004) Why there aren't more information security research studies, *Information & Management*, 41, 5, 597-607.

22. Melara, C., Sarriegui, J. M., Gonzalez, J. J., Sawicka, A., and Cooke, D. L. (2003) A system dynamics model of an insider attack on an information system," in J. J. Gonzalez (Eds.) *From modeling to managing security: A system dynamics approach*, Norwegian Academic Press, Kristiansand, Norway, 9-36.
23. Richardson, R. (2011) 15th Annual 2010/2011 Computer Crime and Security Survey, Computer Security Institute, New York, NY.
24. Siponen, M.T. (2005) An analysis of the traditional IS security approaches: Implications for research and practice, *European Journal of Information Systems*, 14, 3, 303–315.
25. Smith, M. J., and Carayon-Sainfort, P. (1999) "A balance theory of job design for stress reduction, *International Journal of Industrial Ergonomics*, 4, 1, 67-79.
26. Straub, D.W. (1990) Effective IS security: An empirical study, *Information Systems Research*, 1, 3, 255-276.
27. Straub, D.W. and Welke, R.J. (1998) Coping with systems risk: Security planning models for management decision making, *MIS Quarterly*, 22, 4, 441-469.
28. Sterman, J.D. (2000) *Business dynamics: Systems thinking and modeling for a complex world*, Irwin McGraw-Hill, New York, NY.
29. Sunyaev, A., Tremmel, F., Mauro, C., Leimeister, J.M., and Krcmar, H. (2009) A reclassification of IS security analysis approaches, *Proceedings of the 15th Americas Conference on Information Systems (AMCIS 2009),* San Francisco, August 6-9, Paper 570.