International Journal of ASRO
Volume 9, Number 2, pp. 107-114
July-December 2018

INFORMATION SECURITY MANAGEMENT STRATEGY ANALYSIS USING SYSTEM DYNAMICS MODELING

Arie Marbandi[1], Ahmadi[1], Adi Bandono[1], Okol S Suharyo[1]

[1]*Indonesian Naval Technology College, STTAL.*
Bumimoro-Morokrembangan, Surabaya 60187, Indonesia

ABSTRACT

Handling information security management is an absolute thing to do for organizations that have information systems to support the organization's operations. Information systems consisting of assets both software and hardware that manage data and information that are spread over networks and the internet, make it vulnerable to threats. Therefore investment and costs are needed to secure it. Costs incurred for this need are not small, but investment expenditures and information security costs carried out need serious handling to be more effective and on target. The System Dynamics Model is used to evaluate alternative strategies to demonstrate the effectiveness of investment and the cost of managing information security through simulation of policy changes. System Dynamics are methods for describing models and systems analysis that are dynamic and complex, consisting of variables that influence each other in the form of causal relationships and feedback between variables that are either reinforcing or giving balance. Simulation using a dynamic system model in this study illustrates that the management of risk assessment followed by vulnerability reduction efforts has a very large impact on the management of information security. By making a difference in the value of security tools investment, this provides an alternative choice in information security risk management investments to achieve the effectiveness of the overall costs incurred in managing information security.

Keywords: *Information Security Management, System Dynamics, Simulation, Model.*

1. INTRODUCTION.

Managing information security is a very important and challenging task. The organization allows employees and other people to access information systems from everywhere, with the sophistication of increasing security threats, the need to provide security is considered more important. Effective information security management requires security resources that cover a variety of fields, including attack prevention, threat prevention and vulnerability reduction. Using a system dynamics model will provide alternative security management strategies through the viewpoint of investment costs.

Systems Dynamics are used to determine the financial implications of organizational decisions in determining investment information security assets. The ability to correlate construction over a period of time and track progress across time is an important factor in choosing a system dynamics simulation methodology. This model is intended to cover security, vulnerability and attack policies, linking them with ongoing security costs and overall damage. This

model provides managers with the ability to know the influence of resources placing them in alternative security options and the impact of decisions under various conditions. Although the model cannot cover all attacks security and scenarios, the model provides managers with insight into relative risk sacrifices. This research adopts design science methodology using dynamic system models as an interesting discussion. The utilization of the discussion is shown through the successful implementation of the model under various conditions. This study also discusses the management and implications of security model research (D. L. Nazareth, J. Choi, 2014).

The system dynamics methodology approach shows how structures, policies, decisions and time delays with the system are interrelated and influence in growth and stability. It is assumed that system functions are determined by the structure, and the pattern of system behavior depends on the dynamic structure and internal feedback mechanism of the system. The first step to implementing information security management is to develop a complete information security policy (Pei-Chen Sung, Chien-Yuan Su, 2013).

Build a causal circumference diagram with a series of factors identified, and then build an SD model to reveal a risk assessment model, in the form of a simulation that produces five types of risks namely hardware system risk, software system risk, data risk , environmental risk and human risk (Liu Wei, et.al, 2015).

In this research journal will use a system dynamics model for information security management, where modification of the model will be carried out in previous research by looking for leverage variables and adding other variables if needed for further analysis. Information security management modeling can show that simulations using dynamic systems give an overview in the form of construction or structure, in the form of a scenario that is correlated with several important variables in accordance with the problems discussed in this study, namely the management of information security.

Validation is done by making adjusted equations changes according to time, which will then create a basic result according to the scenario. System dynamics simulation modeling for information security management was also developed to be able to analyze information security management strategies by making policy alternatives that could be used as material for more efficient decision making.

2. MATERIALS/METHODOLOGY.

System Dynamics (SD) is a method for describing models and analyzing systems or complex dynamic issues in terms of processes, information, strategies and organizational boundaries (Erik Pruyt, 2013). Systems Dynamic learn about the behavior of dynamic and complex systems in a feedback process that consists of reinforcing and balancing loops (Miroljub Kljajić, et. Al., 2012). A system dynamics was developed in 1950 by Jay W. Forrester of Massachusetts Institute of Technology (MIT). This framework focuses on systems thinking, but takes additional steps to build and test simulation models. A main characteristic of this method is the existence of a complex system, changes in system behavior, and the existence of closed-loop feedback to describe new information about the condition of the system that will produce the next decision. (Erma Suryani, et.al, 2010).

Using a system dynamics model, managers can create "if-then" scenarios by changing variables to see how the system's performance will be changed

and can use that information to manipulate the system to achieve the desired results. (Deborah Marshall, et. Al, 2010).

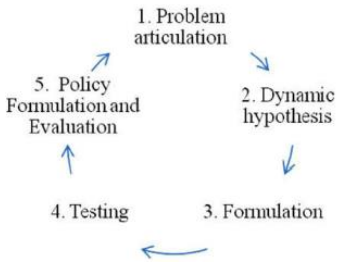

Fig. 1 The Steps To Create SD Model

The basic concept in systems dynamics is that the state of the system is self-modifying state according to the feedback and can be visually described as seen on figure 2 (Dr. Michael Yearworth, 2014).

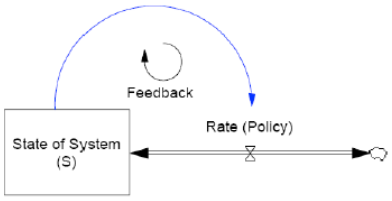

Fig. 2 Self-Modifying State According To Feedback

The rectangle states the stock, the quantity of the system that is the subject that accumulates, and/or the reduction in accumulation according to the level of inflow or outflow indicated by the valve symbol The cloud symbol shows the system boundary. This shows that the source or sinking of the current is outside the system.

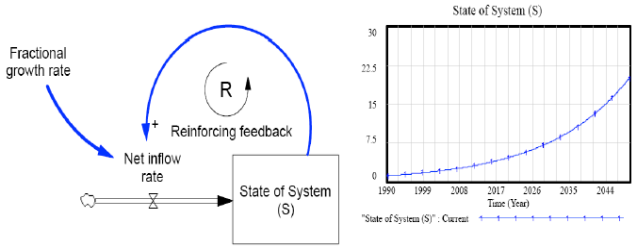

Fig. 3 Reinforcing Feedback Directs to Exponential Growth

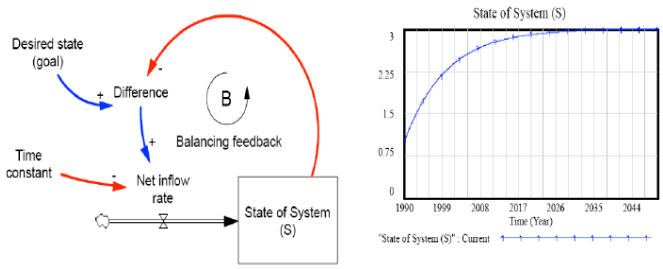

Fig. 4 Balancing Feedback Directs to Achieving Goals

Reinforcing Diagram shown in figure 3 and show exponential growth in the state variable. Figure 4 show behavior achieving the goal of feedback balancing.

3. RESULT AND DISCUSSION.

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 5. We provide a quick overview of the notation. Items in rectangles representstocks 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.

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.

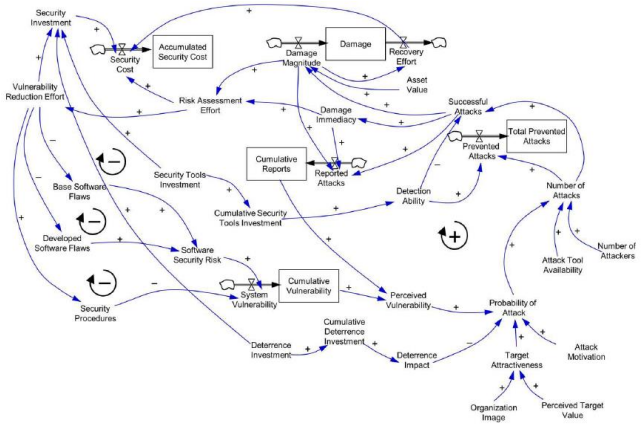

Fig. 5 Information Security Management Model

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 maybe 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.

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.

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 6. 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.

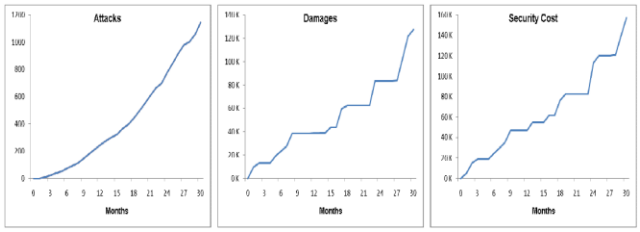

Fig. 6 Simulation Results for Base Scenario

Table 1. Simulation Results for Alternative Security Investments

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

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.

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.

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.

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.

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.

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.

4. CONCLUSION.

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.

5. ACKNOWLEDGEMENTS.

This research has been Supported by Indonesia Naval Technology College (STTAL).

6. BIBLIOGRAPHY.

Ae Chan Kim, Su Mi Lee, Dong Hoon Lee, 2012, Compliance Risk Measures of Financial Information Security using System Dinamics, *International Journal of Security and its Applications*, Vol. 6, No. 4.

Abbas, H., Magnusson, C., Yngstrom, L., dan Hemani, A., 2011, Addressing Dynamic Issues in Information Security Management, *International Journal of Information Management & Computer Security*, Vol. 19 No. 1.

Deborah Marshall, Paul Rogers, Thomas Rohleder, Sonia Vanderby, 2010, System Dynamic Modelling: A Decission Support Tool to Improve Care for HIP & Knee Oesteoarthritis, *Alberta Canada: Institut of Health Economic*.

Derek L. Nazareth, Jae Choi, 2015, A System Dynamics Model for Information Security Management, *International Journal of Information & Management*.

Dr Mike Yearworth, 2014, "*A Brief Interoduction to System Dynamics Modelling*" University of Bristol.

Eric Pruyt, 2013, "*Small System Dynamics Models for Big Issues*", TU Delft Library, Delft, The Netherlands.

Erma Suryani, Shou-Yan Chou, Rudi Hartono, Chin-Hsien Chen, 2010, Demand Secenario Analysis and Planned Capacity Expantion: A System Dynamic Framework, *International Journal of Simulating Modelling Practice and Theory*.

Liu Wei, Cui Yong-feng, Li Ya, 2015, Information System Security Assessment Based on System Dynamics, *International Journal of Security and its Applications* (IJSIA), Vol. 9, No. 2.

Pei-Chen Sung, Chien-Yuan Su, 2013, Using System Dynamics to Investigate the Effect of the Information Medium Contact Policy on the Information Security Management, *International Journal of Business and Management*, Vol 8.

Yang, S., Wang, Y., 2011, System Dynamic Based Insider Threats Modeling, *International Journal of Network Security & Its Aplication (IJNSA)*, vol. 3, No. 3.