The Application of System Dynamics for Managing Information Security Insider-Threats of IT Organization

Farhad Foroughi [#]

***Abstract*—Decision making in mission crucial scenarios is a complex cognitive task involving analysis of numerous variables which are often interdependent. System dynamics has frequently been demonstrated to be an effective analytical tool in a wide variety of situations. System dynamics has frequently been demonstrated to be an effective analytical tool in a wide variety of situations such as the Inside-Threats security problems in IT organisations because the casual factors are dynamic. The security issues in the risk management concern to psychological motivations, the technical process, the business process, awareness methods, the culture and key staff members dynamically. This paper will discuss about the System Dynamics methodology and its relation to the problem by using CLD and Stock-Flow diagrams and will validate the selected model for the problem solving.**

***Index Terms*— Decision Support Systems, Information Security, Insider-Threats, Security Management, System Dynamics.**

I. Introduction

The companies those business on Information Technology (IT) need more attention on information security because their business related to the processing of large amount of information using theoretical knowledge and practical experience. In addition, effective problem-solving requires fast and accurate comprehension and analysis of the issues surrounding the problem. The security of information and information systems is a critical task in these companies and needs more attention on inside and outside threats that may be happened.

Decision making in mission crucial scenarios is a complex cognitive task involving analysis of numerous variables which are often interdependent. One of the most useful models that help in this operation is System Dynamics. System dynamics has frequently been demonstrated to be an effective analytical tool in a wide variety of situations, both academic and practical, and is currently being used by a number of companies. Many of the applications of system dynamics involve the quantitative assessment of the costs and benefits of various programs, both retrospectively and prospectively.

Farhad Foroughi is with *University of Sunderland*

In this paper, the following outcomes will cover:

- Inside-Threats security problem in IT organization
- System Dynamics methodology and its relation to the problem
- Why System Dynamics used in this situation
- CLD and Stock-Flow diagram for the problem
- Validation of selected model for the problem solving.

II. The Problem

The number of security incidents reported by the CERT Coordination Center (CERT/CC) has rose gently each year since last 8 years [1]. In the summery, 27% of security events occurred was insiders. This means according to security incidents those may happen for organization, attention to insiders is primary. In each security incident, 50% of factors may cause by insiders, SANS said.

The casual factors according to this problem are dynamic. The security issues in the risk management concern to psychological motivations, the technical process, the business process, awareness methods, culture and key staff members dynamically.

The problem that should be solved is a model for insider-threats that may happen in organization to manage them to mitigate to an acceptable level of risk.

The definition of an insider threat crime adopted in the USSS/CERT is:

"Any information system, network, or data compromise where the suspect has – or used to have – legitimate access to the network/data compromised." [2] The definition includes suspects who are:

1) Current or former employees of the company whose network was compromised;

2) Current or former contractors of the company whose network was compromised;

III. Methodology

One of the difficulties in systematic modeling of security attacks arise from the unavailability of data regarding these attacks. While such attacks are increasingly familiar on networked systems, systematically collected data on these attacks is not generally available. This shortage of availability stems from three primary causes: Attackers generally act to conceal their attacks; defenders gather data

on attacks for narrow purposes; organizations controlling information assets rarely share data on attacks. [3]

To manage complex systems, a model must be capable of representing systems with all complexes and dynamics components. It should be understandable and usable for managers. The System Dynamics is a good modeling for this problem and is capable to represent the system with all complexes and dynamics characteristics of the problem that shown below:

1. The problem is extremely complex, consisting of multiple interdependent components;
2. The problem is highly dynamic;
3. The problem involves multiple feedback processes;
4. The problem involves nonlinear relationships;
5. The problem involves "soft" data.

IV. SYSTEM DYNAMICS MODEL

The risk management of the insider-threats problem involves a complex combination of behavioral, technical, and operational issues. Insiders may be allowed to bypass all of those measures in order to carry out their daily duties. Former employees are aware with internal policies and procedures, which can also be exploited to facilitate attacks. Insiders can be motivated by a variety of factors. The Financial gain is a common motive in certain industries, while revenge can cover businesses. In addition, theft of intellectual property is prevalent in some sectors, for differing reasons. In all, eighteen variables identified and grouped in 4 categories and listed below: [3]

Detection Procedures	Motive Triggers	Focal Actor in Possibility of Attack	Preventative Policies
Position in company	Employee/ management tension	Trust in employee	Respect for insider
Management attention	Behavioral oversight	Mistreating of fellow employees	Preventive HR procedures
Awareness of risks	Turnover of critical employees	Staff trust	Focal actor job satisfaction
Financial health of organization		Average job overload	Percent of shared organizational knowledge
		Employee access upon termination	Awareness
			Management of technology /data

This is significant to know that some of these variables may move to another category according to some cases and some of them may affect directly and independent to a category. [4]

A. The Causal Loop Diagram

At this level, the causal loop diagram (CLD) explains cause-effect influences by an arrow pointing from cause to effect. Even at this level, the causal loop diagram can qualitatively explain phenomena and avoid the costly mistakes and suggest better measures to manage the system [6].

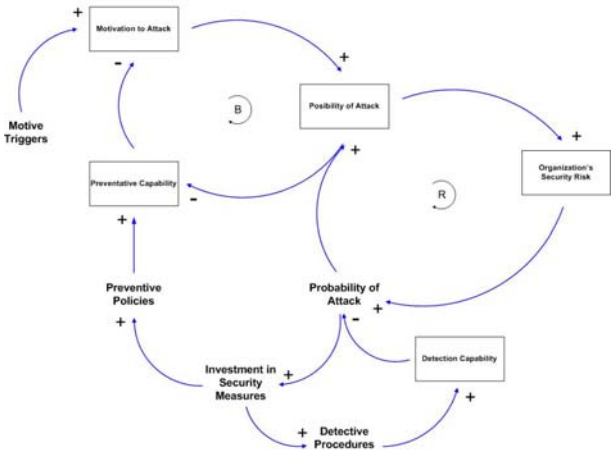

Figure 1. The insider-attack casual loop diagram.

According to the above diagram, motive triggers will increase motivation to attack and increasing in this stock will increase possibility of attack because its capability raises interaction of attack. The Possibility of attack, preventive capability and motivation to attack create a feedback balance loop because increasing in possibility of attack effects on preventative capability and decreases it because it reduces potential and discipline of policies in organization. [4] Decreasing in preventative capability will increase motivation to attack because when no policy or discipline exists, it is a motive trigger for future attacks.

Preventative capability will be increased by preventive policies that applied in organization and this depends on investment in security. This means, good preventive policies need enough investment in security and management support. Investment in security relates to return on it that management requires to know how much of investment will bring back. After any aggression, usually, the top manager is ready to invest money in security because they lost money in the security fraction. Risk management could help them to find how much investment needed [5]. The evaluation of probability of attack and its influence and consequence will help to find how much security investment adequate.

In the other hand, the Possibility of attack effects on organization's security risk because when possibility raised, probability of threat will be going up and risk is threat multiple its probability of occurred. In addition, the security risk effects on probability of attack directly. When the risk increased, probability of attack will rise too but detection measures could reduce it [5]. Detection methods could not prevent attacks immediately but they could effect on it by sending alarm and improving management attention on them.

Finally, the feedback loop between the possibility of attack, the organization's security risk and the probability of attack is a reinforce loop because increasing in each part,

increase another variable too. The probability of attack effects on possibility of attack and will improve it because it avoids security measures and grow vulnerabilities.

B. The Stock-Flow Structure

The stock and flow diagram is a graphically representation of the system and facilitate as a core part of the system dynamics approach. It provides a link to simulation modeling because it helps us assign equation to the relationships between variables. This is very valuable and could make a clear picture of complete system and relation between components [6]. The following diagram created for the insider-attack problem.

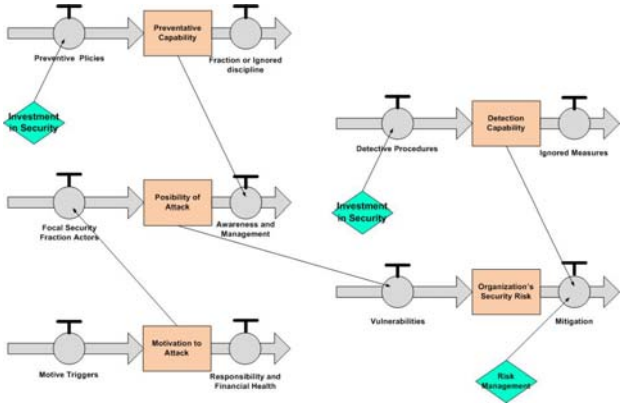

Figure 2. The insider-attack's Stock-Flow Diagram

The diagram describes 4 stocks. The inflow and the outflow explained for each stock. The preventive policies are inflowing preventative capability because those increase its capability but a fraction in discipline or ignored usage of them will decrease that capability [4]. The investment in security is an important variable that could effect on the inflow. The focal security fraction actors are inflowing the possibility of attack because its potential will increase its capability but good and adequate management support and awareness program could decrease that. The preventative capability is a significant variable in according to management support and awareness that means it could describe which program or support required and may control them to best level [5]. In addition, it sounds that the motivation to attack is a key reference for focal security fraction actors that may happen. The motivation to attack controlled by motive triggers as an entry but responsibility and financial health act as the outflow. The culture of responsibility and confidence about financial health in the system will decrease the motivation of attack but its level could effect on focal actors as a feedback reaction.

In other hand, the vulnerabilities increase the degree of organization's security risk but the mitigation that is resulting from a risk management program could manage and balance it. The level of the possibility of attack effects on vulnerabilities directly and this is very clear because that rises break points in the security system. The detection capability is another reference for the mitigations that could grow it up. That is the issue of detection procedures and measures those depend on security investment. This is serious for concern that technology cannot completely detect successful attacks on the complex system. It should be used in the system continual because ignored procedures and measures will decrease the detection capability.

V. Conclusion

After analyzing model behavior during this tutorial, this is found that the System Dynamic is the primary model to be a valuable tool to analyze insider-threats because of its dynamic attributes and soft problem characteristic. A focus on maintenance of essential keys requires a systemic approach that considers the whole range of organizational policies, practices, procedures, and technologies that may contribute to the occurrence of security incidents. Because of nature of the variables and related parameters, the casual-loop diagram and the stock-flow diagram explained behavioral reactions and relationships between components in the system. In this situation, feedback loops are very significant because attackers are a part of system and may motivate with internal signals or may involve on other part of entire complex system.

References

[1] CSO Magazine. (2006, 09, 6). 2006 E-Crime Watch Survey. *CSO Magazine.* [Online]. Available: http://www.cert.org/archive/pdf/ecrimesurvey06.pdf.

[2] D. Cappelli. (2005, 11, 14). CERT-Preventing Insider Sabotage: Lessons Learned From Actual Attacks. *Carnegie Mellon University.* [Online]. Available: http://www.cert.org/archive/pdf/InsiderThreatCSI.pdf.

[3] SEI/CERT. (2004). Preliminary System Dynamics Maps of the Insider & Outsider Cyber-threat Problems Vr. 1.0. *CERT/SEI-The second workshop on system dynamics and cyber security*. [Online]. Available: http://www.cert.org/research/sdmis/cyber-threat-maps.ppt.

[4] M.E. Whitman & H.J. Mattord. (2004) *Management of Information Security*, Canada:Thomson Course Technology.

[5] M.E. Whitman. (2003, 08) Enemy at the gate: Threats to information security, *Communication of the ACM*, vol. 46, no. 8. pp. 91 - 95.

[6] L. Wang & E.Wong. (2007, 05, 26) A Threat Model Driven Approach for Security Testing, *Proceeding of Third International Workshop on Software Engineering for Secure Systems.*

APPENDIX

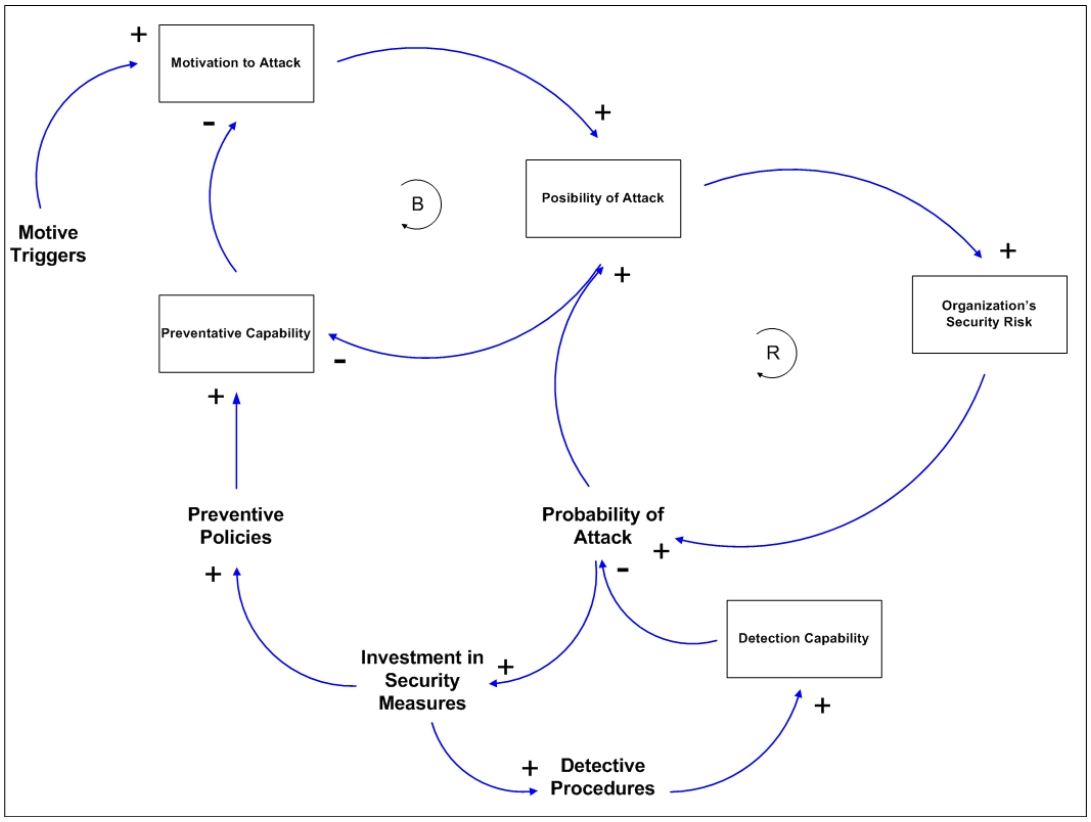

Figure 1. The insider-attack casual loop diagram.

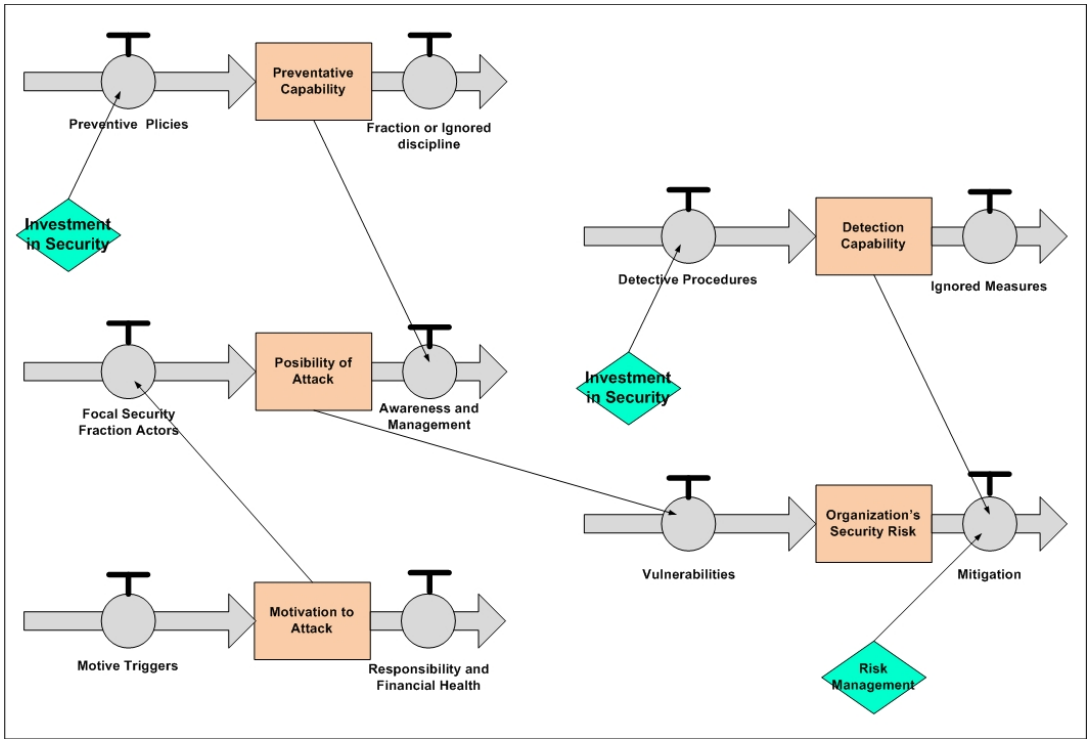

Figure 2. The insider-attack's Stock-Flow Diagram.