Searching for Preventive-Corrective Security Balance

Jose Manuel Torres, Jose Maria Sarriegi, Javier Santos

Tecnun - University of Navarra

Pº Manuel de Lardizabal 13, 20018 Donostia - San Sebastián, (Spain)

Phone: 34943219877 Fax: 34943311442

jmtorres@tecnun.es, jmsarriegui@tecnun.es, jsantos@tecnun.es

Abstract

Organizations are becoming more aware about the importance of economic, financial and risk management aspects of information system security. As a result, the balance between preventive and corrective security strategies must be studied. We understand *Preventive Security* as the ability of organizations to avoid the impact of an incident and *Corrective Security* as the ability of the firm to recover from the losses generated by an incident.

This paper presents a model to analyze the Preventive-Corrective security balance. The main objective of this model is to simulate and analyze the impact that two security behaviors (security investments and strategy) can have one a given enterprise environment. After running 54 simulations, some interesting security behaviors called our attention.

Keywords

Security; Security Management; Preventive-Corrective security strategy balance.

Introduction

Today's technology allows users to download, upload and manage information in an abusive way. These unexpected usages plus unsecured software designs originates information systems window of exposures. As a result, controlling and managing information systems are becoming necessary evils for enterprises. Businesses in their daily routine are dealing with DOS, information losses and unnecessary bandwidth consumptions. They are installing firewalls, antivirus, IDS and many other security products. Organizations are aware about the advantage of information systems but, they must design robust management procedures in order to get the most out of it. The CSI/FBI computer crime and security survey, revealed how organizations are becoming more aware about the importance of economic, financial and risk management aspects of information system security [1]. Nevertheless, only few organizations take into account security level indicators and face the robustness and complexity issues of information systems architectures.

The desire or necessity to interconnect these information systems, internally and externally, increases the complexity of these information systems architectures. The increment on complexity combined with users' misuses also compromise information security. These facts mentioned above, lead us towards the design of a security management simulation model in order to better understand security tradeoffs and decision making. This work seeks to exhibit interesting security management behaviours proving System Dynamics' suitability when dealing with complex problems such as security management.

Protection Strategies

Some security experts highlight detection and mitigation mechanisms as the road towards organizational security [2]. Others recommend approaching security from preventive and corrective perspectives [3]. Bruce Schneier, considered today a worldwide security reference, identifies three stages for information systems security improvement: prevention, detection and response. Schneier among many other security experts has been predicating the necessity of moving from technical security to managed security. Neither traditional security products are enough to ensure organizational security nor security models designed to avoid threats [4].

Organizations need security models which help them to understand organizational risk as a part of doing business. These business oriented models should also help them to reduce risks by implementing proper technical, formal and informal security controls, leading them towards risk sharing with other parties such as contracts or insurance [5],[6].

In order to do so, a balance between preventive and corrective security strategies must be studied. There have been studies about how to find optimal balance between preventive and corrective security strategies [3]. Nevertheless, organizations have been trying to minimize risk and secure information systems by focusing on security equipment. Finding this balance could represent a good starting point towards achieving higher levels of organizational security.

Information systems security should not be only based on preventive actions. Optimal information systems security can be achieved by including detection and efficient and fast incident response. The following work, presents a security simulating model that reflects how we understand security of information system. This security model attempts seeing security from a managerial point of view while analyzing two management approaches: *Preventive Security* (processes and procedures to prevent and detect incidents) and *Corrective Security* (response after the incident). These definitions will be further developed throughout the paper.

Preventive Security

For some firms involves in the security business, preventive security is about monitoring, capturing, analyzing and reporting suspicious activities. According to these security firms, preventive security allows organizations to identify and assess new vulnerable areas of the system and measure the effectiveness of current security solutions [7]. No one doubts that preventive security mechanisms such as firewalls, antivirus scanners, cryptology, digital signatures, protocols and many others tools provide a barrier that protects the systems against intrusions.

Implementing preventive security is not as easy as one can think. In order for it to be effective, used technologies must spot new or known incidents in real time. These incidents must be spotted before they succeed and these technologies must be accurate enough to avoid false negatives (failing to spot an incident) as well as produce small amount of false positives (false alarms) [8].

After reviewing security literature, and comparing security experts' opinions, for the purpose of this security model, we will define *Preventive Security* as the ability of organizations or firms to avoid the impact of an incident. In other words, the resources invested in prevention and detection efforts. That is, from time zero (implementation of technical, formal and informal controls) [9], to the time when the attack is perceived (detection).

$$\boxed{\text{Preventive Security} = \text{Time} = T_{\text{Attack}}}$$

Corrective Security

Corrective security actions are as important as preventive actions. Information systems highly depend on software and hardware design robustness. Just by taking software development as an example, it is possible to realize how time-to-market impedes software security testing procedures, and therefore, in any piece of software more than one vulnerability can be found. Software developers do not take into account incorrect installations and malicious or unexpected uses [8]. In these cases, corrective actions can be very useful. In software maintenance, corrective actions are utilized to identify and remove faults in the system. Similar approaches would perfectly work when securing information systems [10].

Corrective security mechanisms such as backups and contingency plans are evidence in the necessity of corrective security strategies [11]. Corrective security throughout this work will be defined as the ability of the firm to recover from the losses generated by an incident. That is, the processes and procedures to follow right after the attack (Incident response).

$$\boxed{\text{Corrective Security} = \text{Time} > T_{\text{Attack}}}$$

Objective

The main objective of this model is to share the way we understand security from a preventive and corrective point of view. This paper highlights the importance for organizations to find a balance between these two security approaches. Furthermore, offers a modeling approach that allows simulating and analyzing the impact that two security decision making behaviors (1 & 2) can have on a given environment (3):

1) Investments on security: Relaxed, Intermediate, Sensitized.

2) Security management strategies: Corrective focused, Preventive focused and Even.

3) Enterprise Environment: High, Medium, and Low incidents rate.

In addition, this model represents an opportunity to create a common modeling language, motivating people to simulate, alter inputs, make comments and see the importance of structure when trying to understand the behavior of a complex system.

Preventive-Corrective Security Model

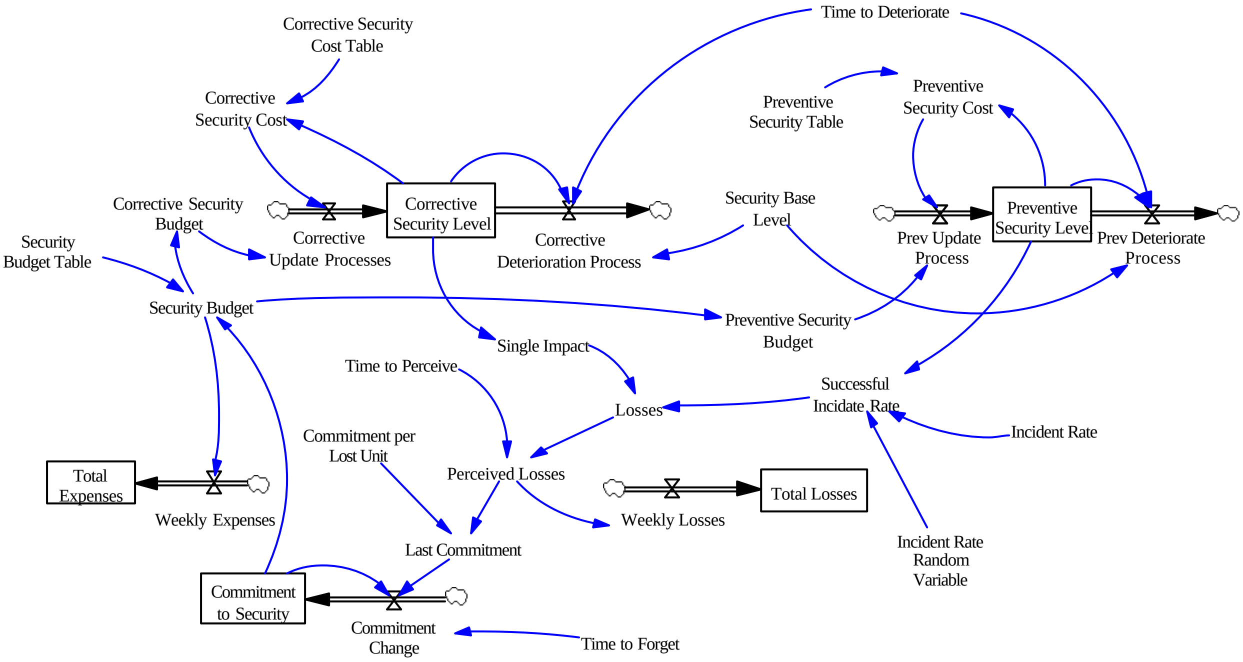


Figure 1: Preventive-Corrective security model

The presented model (figure 1), has the following levels:

- *Corrective Security Level*: The higher the corrective security level, the lower the *Single Impact* variable will be. For example, with a *Corrective Security Level* of 0.7 (on a range from 0 to 1), and an incident magnitude of $18000, the real losses generated by it will only represent 30% of the magnitude of this incident. ($5400)
- *Preventive Security Level*: The higher the preventive security level, the lower the *Successful Incident Rate* will be. For example, with a *Preventive Security Level* of 0.8 (on a range from 0 to 1), only 20% of the incidents generated by the *Incident Rate* variable are going to be able to penetrate the system (which can be translated as losses.)
- *Total Losses:* Accumulated losses (in $) due to incidents.
- *Total Expenses:* Accumulated investments (in $) on preventive and corrective security.
- *Commitment to Security:* Degree of management's compromise with security.

There are two relevant variables:

- *Successful Incident Rate:* Number of incidents unable to stop, which generates losses.
- *Single Impact:* Impact of the incident if it actually happens.

Accepted-Assumed Hypothesis

- *Commitment to Security:* the only factor that makes management more committed to security is firms' direct losses. (i.e. direct impact, not external security incidents news, neither lost of reputation, etc)
- *Losses:* They are measured in American Dollars. For the purpose of the model, we do not differentiate between all different types of losses (viruses, information losses, reputation, etc.)
- *Losses perception:* all losses are perceived by management regardless and with a 4 weeks delay.
- *Security Level:* The higher the security level becomes, the heavier the investment has to be in order to increase the security level.
- *Incidents Rate***:** They are randomly generated and do not depend on any variable or external factor.
- *Incidents:* Incidents' natures are not distinguished. We simplify incidents as negative economic impact. (- $)
- *Preventive Security Level Action:* Incident halt or success (to stop it or not) does not depend on the incident's magnitude. It depends on the preventive security level. (The higher the preventive security level, the fewer incidents will go through the system (*Successful Incident Rate* reduction))

Security Scenario

For our first simulation (figure2), the Preventive and Corrective Security levels have the same value (0.5**Security Budget*) therefore, these two strategies go one on top of the other. In the graph presented below, there are incidents (blue) "losses" randomly happening throughout 100 weeks with different magnitudes. During the first 18 weeks, the commitment to security as well as the security budget slightly decreases (management relaxation). However, when the first incident (blue peak) on week 20 occurs, these incident or loss is perceived 4 weeks later. As a result, the commitment to security increases as well as the security budget. This scenario may look common sense type. Nevertheless, the important contribution of this work is when the Total Security Budget favors one strategy or the other. Then, the results obtained from this change in the preventive and corrective balance generates interesting counterintuitive security scenarios that will be presented.

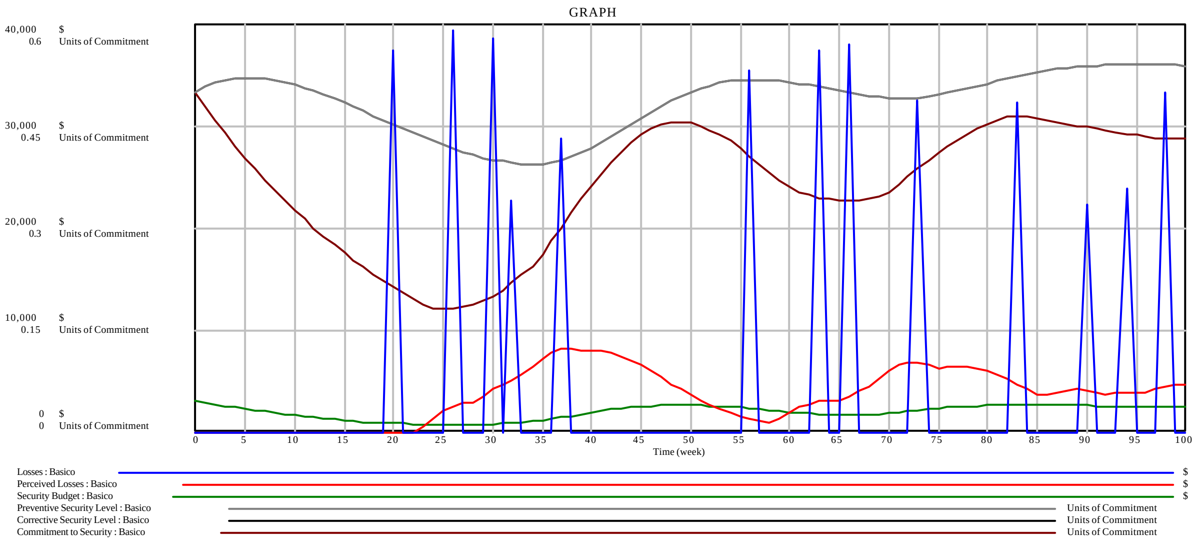


Figure 2: Simulation of the Initial State (from week 0-100)

Simulated Scenarios

In order to develop and illustrate what we believe are significant security scenarios, the following sets of behaviours and scenarios have been executed based on two main policies while changing the incident rate:

Management Decision Making:

- *Relaxed:* Not preoccupied about security issues and therefore the investments on security are minimum.
- *Intermediate:* Slightly preoccupied about the budget dedicated to security. Therefore, it is somewhere in between those policies. (Relaxed and Sensitized)
- *Sensitized:* Very preoccupied about security and so, there are large investments on security.

Management Perception of Security Needs:

- *Preventive Focused:* Management oriented towards prevention of incidents. I.e. 70% of the security budget dedicated to preventive strategies and 30% to corrective strategies.
- *Corrective Focused*: Management in favor of correcting incidents after happening. I.e. 70% of the security budget dedicated to corrective strategies and 30% to preventive strategies.
- *Even:* Half of the total security budget for each strategy. (50% preventive, 50% corrective)

Enterprise environment:

- *Low Incident Rate* (8 incidents in 100 weeks),
- *Medium Incident Rate* (19 incidents in 100 weeks)
- *High Incident Rate* (36 incidents in 100 weeks)

Results

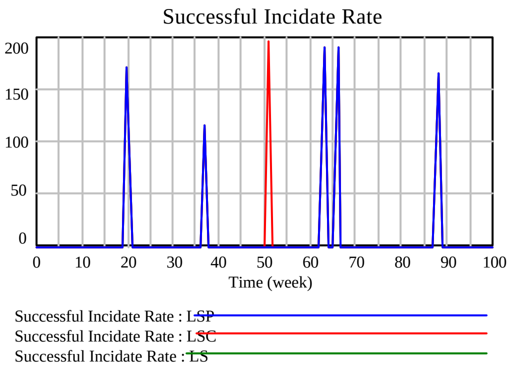
After Running 54 simulations (Figure 3) combining all possible scenarios, some interesting security behaviors called our attention:

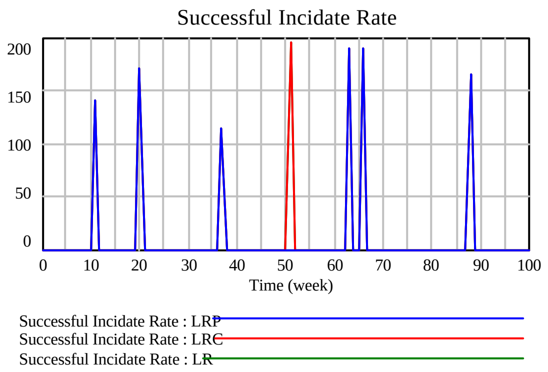
		Relaxed		Intermediate		Sensitized	
		Expenses	Losses	Expenses	Losses	Expenses	Losses
Low Incident Rate	Preventive Focused	79729	293963	126175	227152	216111	184948
	Even	85348	305448	135905	238408	197326	161152
	Corrective Focused	78135	279835	132340	233590	217262	179536
Medium Incident Rate	Preventive Focused	144512	482546	221723	394030	301610	267142
	Even	123855	429908	193427	346880	321500	290256
	Corrective Focused	135601	457593	200147	363661	295777	268182
High Incident Rate	Preventive Focused	216434	566193	314706	440001	364673	298550
	Even	204988	570542	280211	410903	405901	322520
	Corrective Focused	212471	600888	310994	464166	442852	357117

Figure 3: Data obtained from Simulation

- As it is expected to be, on one hand, relaxed enterprises invest small amount of $ on security and therefore experience large losses. On the other hand, sensitized enterprises invest a large amount of $ on security and their losses are smaller than the relaxed enterprises.
- When the incident rate is low, the losses and the expenses are low. If the incident rate is high then, losses and expenses increase.
- Now the interesting policy to point out is when the enterprises have more corrective oriented security strategies or more preventive oriented security strategies. (See graphs below)

It is interesting to see in the graphs below how the more sensitized strategy is able to stop the incident on the 10th week. It is even more fascinating how the Preventive Security Level of the Relaxed Management strategy stops the incident on the 55th week. Nevertheless, the Sensitized Management strategy is able to stop the same incident not only with its Preventive Security Level but also with the “Even” strategy proving that a more sensitized Management can definitely avoid more incidents from happening.





LSP= Low Incident Rate/Sensitized management/Preventive

LRP= Low Incident Rate/Relaxed management/Preventive

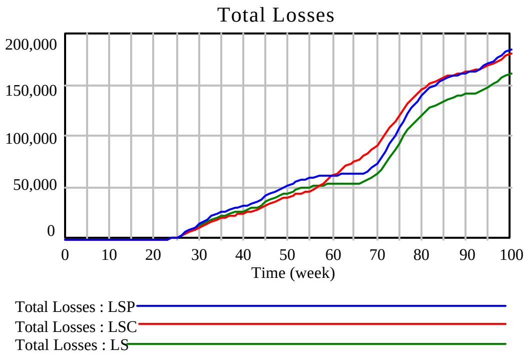
LS= Low Incident Rate/Sensitized management

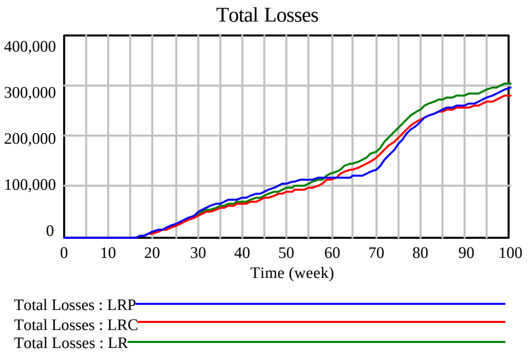
LSC= Low Incident Rate/Sensitized management/Corrective

LRC= Low Incident Rate/Relaxed management/Corrective

LR= Low Incident Rate/Relaxed

From a Total Losses point of view, (see Total Losses graphs) these three policies (Even, Preventive and Corrective) up to the 54th week, have suffered the same number of incidents. The policy with fewer losses is the corrective focused policy due to the fact that it is able to recuperate faster right after an incident (higher corrective level). Therefore, its losses, expenses/budget and commitment to security are inferior. In the “Relaxed Management”, it is important to realize that when they suffer the incident on the 50th week, the losses of the Preventive strategy stay constant (week 55-67) while the Even and Corrective policies keep increasing because the incident causes them more losses, increase their commitment to security and also their security budget. In the “Sensitized Management”, both the Preventive and the Even strategies are able to avoid the 50th week incident.





Conclusions

This security model is able to reproduce both the simplest security behaviours (higher investments, fewer losses) as well as more counterintuitive ones (Preventive Focused strategies vs. Corrective Focused). The model is simple enough to understand without major difficulties and can be used to show system dynamics’ usefulness to non SD initiated people. By evaluating and taking into account these security behaviours, the cost of no security can be more appreciated and better security methodologies can be developed. The absence of real data could be a problem. However, the validity of this model allows us to better understand the root of the causes that generate these security behaviours.

References

1. Gordon, L. A., Loeb, M. P., Lucyshyn, W., Richardson, R., 2004 CSI /FBI Computer Crime and Security Survey, Computer Security Institute Publications

2. Andersen, D., D. Cappelli, J. Gonzalez, M. Mojtahedzadeh, A. Moore, E. Rich, J. M. Sarriegui, T. Shimeall, J. Stanton, E. Weaver, A. Zagonel. (2004). Preliminary System Dynamics Maps of the Insider Cyber-Threat Problem. System Dynamics Society Conference. Oxford, UK.

3. Strbac. G, Ahmed. S, Kirschen. D, Allan. R. 1998. A Method for Computing the Value of Corrective Security. http://www.umist.ac.uk

4. Bruce Schneier. Managed Security Monitoring. http://www.counterpane.com/window.pdf

5. Dhillon G., J. Backhouse (2001): Current directions in IS security research: towards partner-organizational perspectives. Info Systems Journal (11) pp 127-153

6. Dhillon G. (1999): Managing and controlling computer misuse. Information Management and Computer Security (7) 4 pp. 171-175

7. Preventive Security Manager. www.vericept.com.

8. Wimer. Scott. Human Errors Create Security Holes. http://www.theiia.org

9. Torres, J. M., Sarriegi, J. M., 2004, Dynamic Aspects of Security Management of Information Systems, Proceeding of the 22nd International Conference of the System Dynamics Society, Oxford (UK)

10. Dorfman. M, Thayer. R, Software Engineering. 2000 IEEE computer Society.

11. ISO 17799. International Information Systems Security Standard

12. Bosworth S., M. E. Kabay. (2002). Computer Security Handbook. 4 ed. New York, NY: Wiley.

12. Ross, A. (2001). Security Engineering. New York, NY: John Wiley& Sons, Inc.

13. Schneier, B. (2003). Beyond Fear. 1 ed. New York, NY: Copernicus Books.

14. Sterman, J. D. (2000). Business Dynamics. New York, NY: Mc Graw-Hill Companies.