Table of Contents

Go Back

Business Dynamics Based Template Model For Security Policy Management

Denis Trček
Department of digital communications and networks
”Jožef Stefan” Institute
Jamova 39, 1001 Ljubljana
SLOVENIA
denis.trcek@ijs.si

Abstract. During recent decades a great part of efforts for provision of security in information systems was focused on technology. Although it was noted in the eighties that human factor plays an important role, it is becoming evident only now that it plays a central role. Ensuring appropriate security for information systems thus requires not only addressing of technology, but at least as much human and organization related issues. These are usually embodied in security policies, thus the paper focuses on the latter and a model is presented that is intended to support security policy management. The model is based on business dynamics.

Keywords: security, security policy, human factors management, modeling.

1 Introduction

Security issues in information systems have an extensive history. It all started in the sixties with concentration on cryptographic algorithms and secure operating systems. Afterwards, the mid-eighties came, marked by the proliferation of computer communications, which gave importance to cryptographic protocols and security services in general. Approximately at this time, human factors started to be addressed, where a notable example is U.S. DoD Orange Book [US DoD 1983]. This presents one of the first examples of paying attention to human factors that gained further importance in the nineties with the penetration of internet into the business environment. The wide proliferation of e-business exposed security issues form another perspective, which is tight coupling of business processes with IT. This consequently shifted emphasis towards organizational and human resources related issues. It became clear that these elements are probably more important as the classical, technological ones, which is also reflected in the literature [Schneier 2000], [Denning 1999].

Security policies became a standard practice in the business environment. These policies expose the whole complexity of IS security and recently they became a subject of standardization; the basic standard in this area is BS 7799 [BSI 1999]. According to this standard, we will refer to security policy as ways to ensure information confidentiality, integrity and availability. Related goals can be accomplished by a complex interplay between technological solutions and organizational issues. Moreover, today’ s security is also a matter legislation, dependency and other issues [Trček 2003], but this exceeds the scope of this paper.

Now how can one cope with security in IS? Formal methods used to play (and still play) an important role e.g. Z language [Spivey 1989], or logic BAN [Burrows et al. 1990]. As these methods are mostly based on discrete math and logic, they are not sufficient for holistic treatment of IS security, where one needs to model information flows, their perception, the complex interplay between IT and humans, etc. And this is where business dynamics can come to its full potential [Sterman 2000].

2 A model template for IT security management

Business dynamics is a methodology of a quite general applicability to socio-technical systems that information systems in essence are. By concentrating on use of business dynamics for security and having a look at the literature, there is still a long way to go as, and business dynamics has a lot of potentials here. It is worth to mention that some pioneering attempts already exist and they present a promising approach [Gonzalez 2003]. But in general, use of business dynamics in this particular field is rather new.

In this section we will present a template model for security policy management. The model is intended to provide a basic insight and understanding of security policy management related issues. Further, it is anticipated that this model can serve for proper enhancements, i.e. it can be tuned to particular needs, by grounding it on the data from their real business environments. The model includes essential variables, such as threats, perception of threats, i.e. adaptation processes, intensity of security related tasks and security policy levels. The simulations of this model will be deterministic, i.e. no variables will be of a stochastic nature. This is done intentionally to better present the main patterns and behavior of the system. Of course, stochastic variables can be used and sensitivity analysis performed, which is especially necessary for risk analysis. In our model, this can be currently enabled through a variable called plausibility level, which serves to compensate for simplified threats modeling. It is used to model a fact that two IS are not likely to be attacked at the same time, or one is attacked while the other one remains untouched.

We start the modeling with human perception and threats, where human perceptions are certainly very challenging part. They are often modeled as adaptive learning processes with exponential smoothing, called also adaptive expectations. In adaptive expectations, the rate of change in a perceived value X^* is given by a first order, linear differential equation $dX^*/dt = (X - X^*)/D$, where X is the reported input variable (current value), while D is a time constant, called adjustment time. It follows from the literature that adaptive expectations mostly outperform other methods for forecasting [Makridakis 1986] and that is the reason for including them in our modeling process. It should be emphasized that we are aware of the problems related to modelling behaviour, but this exceeds the intention and the scope of this paper.

Next, belief about threats is modeled as a stock, because perception is a state of mind which remains unchanged unless there is a reason to change it. In case of adaptive expectations this change is the discrepancy between real and perceived value.

As far as threats (THR) are concerned, it is evident to an expert that this is a very challenging issue that requires a lot of additional work, but for the purpose of our model we will simplify this issue. Threats will appear at a certain rate, and once appeared, they will remain on the scene for a certain period of time. These threats cease sooner or later due to improved organizational procedures, or new software patches etc. But in a general case that will be addressed in the future, new risks should be added to existing ones and the rate of newly generated risks should be decoupled from the rate of risk extinction. This means that, qualitatively speaking, risks are to be modeled as accumulators. Further, threats modeling should also address exposure time of IS to threats, installed base that is vulnerable to certain threats, etc. In our case it will be assumed that a fixed number of risks is generated at the beginning of the first simulation increment unit, i.e. day. It is further assumed that attackers that are behind those risks (bug finders) have limited capabilities, i.e. that people perform attacks at a constant rate, which means that they successfully attack a certain number of systems per day. This situation lasts for a certain time, when a patch is released and it is assumed that all organizations install this patch immediately. Risks then cease, when another cycle begins with the set of newly discovered vulnerabilities in software.

So, after dealing with threats that are in the heart of the model, the second basic variable is perceived risk (PR), which denotes the number of threats that employees believe in. The discrepancy between PR and THR drives the rate of adaptation, i.e. change in perceived risk (CPR). Certainly, internal accident frequency (IAF) is influenced by PR - the higher the perception of threats, the more intensive are the efforts of the personnel to block threats.

Next, we have to model the main lever, which resides in the hands of the management. This is security policy level (SPL) that is independently driven by corrective intensity (CI). SPL is another external factor that drives change in perceived threats. Additionally, CPR is driven by real adjustment time (RAT) that is further divided into intrinsic adjustment time (IAT) and length of normal operation (LNO). Why this? Because RAT depends on particular circumstances. Let us assume a longer period without accidents. Now when a new accident takes place, expectations are based on past experiences, and people are likely to perceive this event as an isolated one. It is the opposite situation if one experiences attack after attack for a longer period of time. This will lead a person to assume a similar frequency of accidents when the next strike takes place, even if this one belongs to the beginning of a period with a smaller frequency of attacks.

And finally, there are two delays to model the fact that security policy level and discrepancy are always subject to delayed information. The whole template model is presented in Fig. 1.

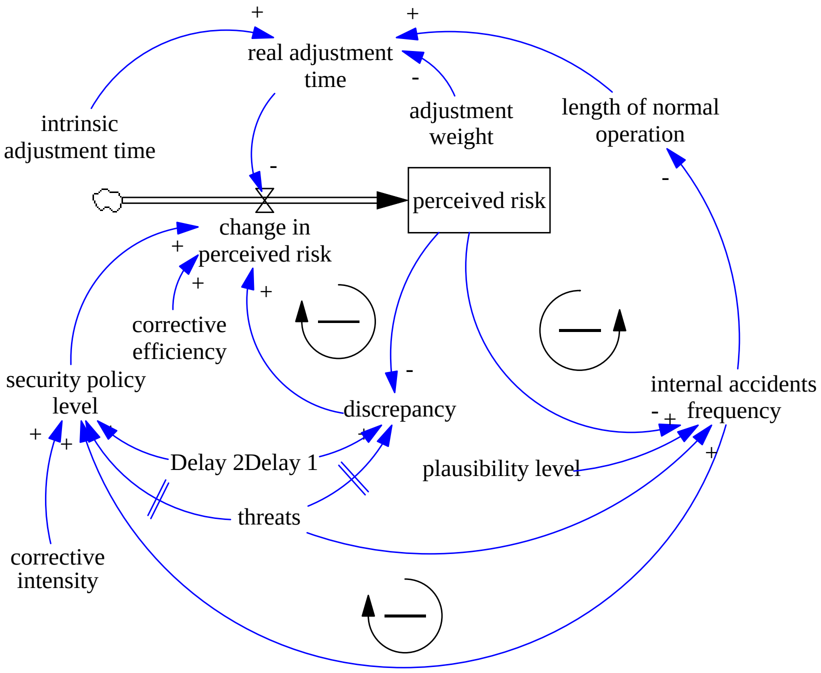

Figure 1: A template model for security policy modeling.

We can also analyze the model from the loops perspective. There are three balancing loops. The upper left loop is the loop of perceived risk (PR, discrepancy, CPR). There is a trust loop in the upper right corner (PR, IAF, LNO, RAT, CPR). It represents the trust of employees in the system according to experienced operational patterns, which influence RAT. The last one is the adjustment loop (PR, IAF, SPL, CPR). It is positioned at the bottom and it models adjustment of perceived risk caused by the management through SPL.

The basic premise of the model is that breaches should decline, if threats are properly perceived - this requires their perception in a timely manner and punctual perception of their quantity and nature.

3 Simulation and analysis

The intention of simulations in this section is to study general patterns of the modeled system. The reasons is that every model has to be tuned appropriately to a specific environment on the basis of real data. This may require modifications to existing functions in the model, or inclusion of additional factors and parameters.

According to the explanations in previous section, the generator of the whole behavior are threats that are modeled with a narrow pulse sequence (a rough approximation for a series of Dirac delta functions). The period for all simulations is 20 days. Attacks appear every day with a frequency one per day. If possible, factors or parameters are set to initial values. This means PR is set to two, while all other variables are set to 1.

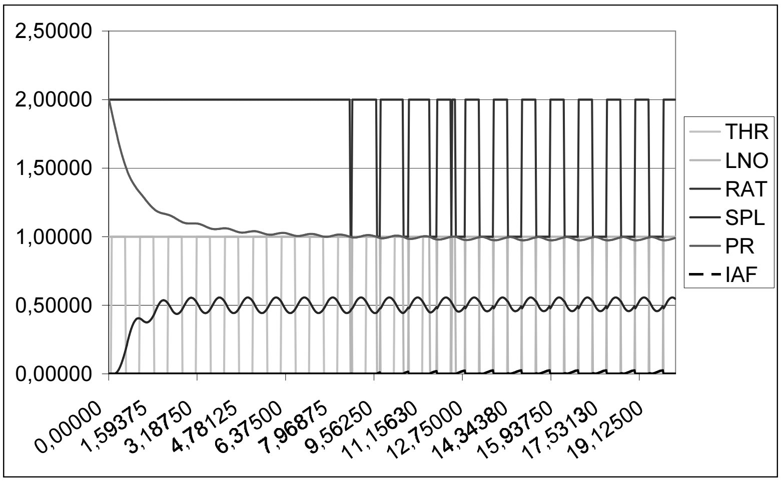

Figure 2: System behaviour with initial values.

The simulation reveals that using initial conditions, there is a transition period of approx. 4 days before the system reaches equilibrium. This is the time needed for the human factor to adjust PR to real threats. One can also note lightly oscillating security policy level, which is not a desired effect, as permanently changing orders lead to resistant behavior of employees. The situation is presented in Fig. 2.

Let' s see what happens if there is a delayed propagation of information about successful breaches, i.e. if we delay the inputs to discrepancy and SPL (see Fig. 3). As expected, delays increase the rate of successful breaches (see the dashed line) and the system reaches equilibrium only after approximately 8 days. In the meantime there are stronger oscillations of SPL, which disappear after this period. This means that the system is oversensitive in terms of reaction at the beginning due to strong change in PR.

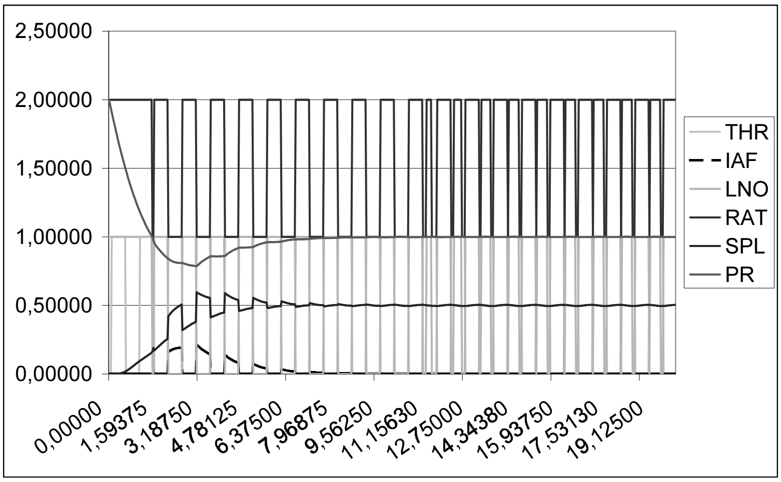

Figure 3: Simulation results with increased values of information delays (Delay 1 and Delay 2).

Now what happens in case when employees adapt slowly to changes? This requires high values for RAT (see Fig. 4). It is anticipated that this will reduce initial over-sensitivity of the system and the simulation approves this expectation.

Finally, let the security manager investigate the influence of increased corrective intensity and, consequently, SPL. Put another way, suppose that security manager tries to find an answer if he / she can eliminate the rest of successful attacks by appropriate driving of SPL. The answer is - yes. It pays off to report to security administrators initial values for threats that are slightly higher than the real ones (see Fig. 5). Practically all oscillations are eliminated and the system is gradually driven from its initial conditions to a desired state. It should be emphasized that IAF has small values and its dashed line is hardly noticable in the diagrams.

The reader should note that the model is valid only within a certain range of given variables - in this case large initial values would cause employees to underestimate threats, if they discovered afterwards that they were reporting too high initial values.

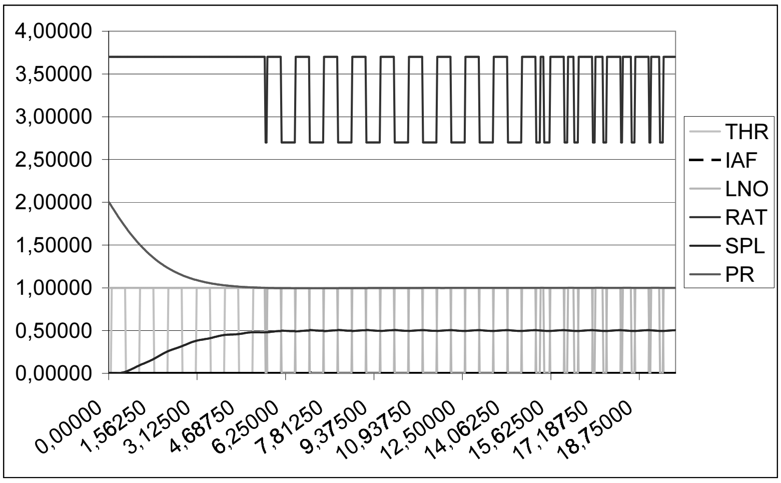

Figure 4: Simulation results of larger IAT values.

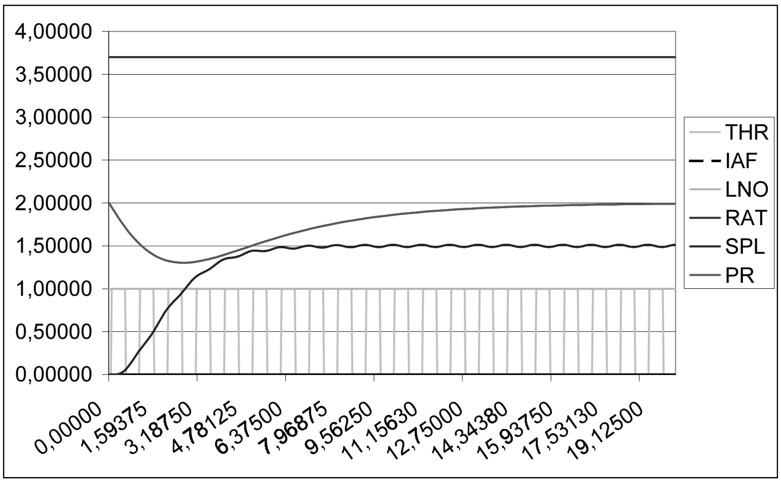

Figure 5: Simulation results of increased SPL through CI.

4 Discussion, conclusions and further directions

It has become evident during recent years that the most important factor behind ensuring security is human factor. In each IS we are faced with a complex interplay between technology and human factor. Thus appropriate methodologies should be used that enable researchers and practitioners to address these issues with more rigor.

Business dynamics turns out to be the right candidate methodology to address these issues. The paper provides such an attempt with a template model for managing security policy in real ISs. Results of deterministic simulations were presented and discussed. Of course, stochastic variables can be used as well in simulations of this model. In the particular case of the presented model, stohastic input has been used to IAF to model the fact that among similar IS with equal weaknesses not of all will be attacked at the same time, some of them will even not be attacked at all. As expected and as observed through simulations, the general patterns on a large scale are preserved, while on a smaller scale responses seem random. With regards to random, chaotic behavior, a reader should be warned that it happens often to inexperienced modelers to conclude that a model enters into chaotic mode at a certain point, but the real cause is caused by the simulation process itself, e.g. due to integration error.

Certainly, the approach in this paper is only one of the early attempts to use system dynamics for IS security. A lot of work in modeling of security is yet to be done. The minimum required is to tune the model to each particular environment, which is achieved through validation that is based on concrete data. But author is aware of the fact that intensive work is required to obtain complete reference sub-models or business dynamics based building blocks for support of security in IS. It is authors belief that this is possible, but only within a wider initiative of experts from various fields.

References

British Standards Institute 1999. *Code of practice for information security management*. British Standard 7799. London: 1999.

Burrows, M., Abadi, M., Needham, R. 1990. Logic of Authentication. *ACM Transactions on*

Computer Systems, 1(8):18 - 36.
Denning D.E. 1999. *Information Warfare and Security*. Addison Wesley: Boston.
Gonzalez, Jose J., ed. 2003. *From Modeling to Managing Security: A System Dynamics Approach*. Vol. 35, Research Series. Norwegian Academic Press: Kristiansand, Norway. www.hoyskoleforlaget.no
Makridakis, S. et al. 1986. *The Forecasting Accuracy of Major Time Series Methods*. John Willey & Sons: Chichester.
Schneier B. 2000. *Secrets and Lies: Digital Security in a Networked World*. John Willey & Sons: New York.
Spivey, M. J. 1989. *The Z Notation: A Reference Manual*. Prentice-Hall: London.
Sterman J.D. 2000. *Business Dynamics*. McGraw Hill: Boston.
Trček D. 2003. An Integral Framework for Information Systems Security Management. *Computers & Security*, 4(22):337-360.
US Department of Defense 1983. *Trusted Computer System Evaluation Criteria*. DoD standard CSC-STD-00l-83. 1983.

Appendix

This appendix gives a complete list of equations that are used in simulations described in this paper. The model has been simulated with $Vensim^{TM}$ package with the simulation increment set to 0.03125 weeks with total duration of 20 days:

- adjustment weight = 1
  units: dimensionless

- change in perceived risk = (discrepancy + corrective efficiency * security policy level) / real adjustment time
  units: accident / (day*day)

- corrective efficiency = 1
  units: accident / task

- corrective intensity = 1
  units: task / accident

- Delay 1 = 1
  units: day

- Delay 2 = 1
  units: day

- discrepancy = SMOOTH3(threats, Delay 1) - perceived risk
  units: accident / day

- internal accidents frequency = IF THEN ELSE(RANDOM UNIFORM(0, 1, 0) $\geq$ plausibility level, MAX((threats - perceived risk), 0), 0)
  units: accident / dimensionless

- intrinsic adjustment time = 1
  units: day

- length of normal operation = IF THEN ELSE(internal accidents frequency > 0, 0 , 1)
  units: day

- perceived risk = INTEG (change in perceived risk, 2)
  units: accident / day

- plausibility level = 0
  units: day

- real adjustement time = intrinsic adjustment time + (length of normal operation / adjustment weight)
  units: day

- security policy level = corrective intensity * (SMOOTH3(threats, Delay 2) + internal accidents frequency)
  units: task / day

- threats = PULSE TRAIN(0.1, 0.5, 1, 20)
  units: accident / day

Back to the Top