SYSTEM DYNAMICS BASED APPROACH TO RISK MANAGEMENT FOR SECURITY IN INFORMATION SYSTEMS

DENIS TRČEK
Department of Communication Systems – E6
»Jožef Stefan« Institute
Jamova 39, 1000 Ljubljana
SLOVENIA

Abstract: Security in information systems is becoming a well-established discipline, where each and every security related activity has to start with the basics. This is risk management. Put another way – risk management is involved in the heart of every security activity. Although risk management is a known discipline in many other areas, its direct translation to information systems is not straightforward because of specifics of contemporary information systems. Among these are the global connectivity of information systems, the number of elements (e.g. thousands of software components), strong involvement of human factor, almost endless possible ways of interactions, etc. Thus a new methodological approach is presented in this paper that is based on business dynamics. It enables the above-mentioned elements to be addressed, improving decision making in information systems security.

Keywords: information systems, security, risk management methodologies, systems theory, system dynamics, simulations.

1. Introduction

During the last decade security of information systems came to the forefront, due mainly to the strong penetration of the internet into all segments of our lives. This new kind of infrastructure that was added to formerly unconnected computers resulted in new security dimensions. Threats emerged that were not known before this era, or were at least of no concern. Of course, protecting isolated computers at the level of local operating systems is one problem. Protecting computers that are globally connected is a very different, and much harder problem.

But there is another issue related to contemporary information systems that is maybe even more important than just protection of devices as such. Recently, "the new economy" exposed the growing importance of non-tangible assets that are at the heart of business processes. Data certainly play a special role here.

Therefore the name of the game in contemporary information systems is data protection. And this results in new demands about security issues, and consequently risk management.

2. Risk Management Basics

One of the earliest definitions of security that is still very useful is the one from ISO 7498-2 standard [6]. It states that security means minimization of vulnerabilities of assets and resources. Further, vulnerabilities mean any weaknesses of a system that could be exploited against the system or data that reside on the system.

The problem with valuation of data is very complex. Not only it is hard to identify all the data, which range from records in databases to company e-mails, but also to value these data. It is interesting to note that, despite the fact that data are becoming identified as one of key assets in organizations, it is not recorded and valued in balance sheets, and it is hard to get insurance arrangements for this purpose.

But the problem is even more complex and it does not stop with the data. Another key ingredient is the employees. This asset is widely recognized as the most important in each and every organization, and also in the area of information systems security. By its very nature (and because of ethical reasons), this asset is hard to value. So for the two basic kinds of assets (personnel and data), efficient risk management remains a difficult issue.

As already mentioned, at the heart of each and every security game there is risk management. The core elements of risk management are assets and threats to these assets. Their interaction results in risks on the basis of assets' vulnerabilities. How much risk an organization is willing to take is a matter of security policy. On its basis countermeasures are taken to neutralize or eliminate risks.

A usual approach goes as follows. Starting with a set of assets $A = \{a_1, a_2, ..., a_n\}$ and a set of threats $T = \{t_1, t_2, ..., t_m\}$, a Cartesian product is formed A x $T = \{(a_1, t_1), (a_2, t_1),..., (a_n, t_m)\}$. For each asset its value $v(a_n)$ is determined, while for each threat related to this asset a probability $E_{a^n}(t_m)$ of interaction during a certain period is determined. On this basis, risk R is calculated as follows: $R(a_n,t_m) = v(a_n) * E_{a^n}(t_m)$.

This procedure is not yet complete. One should be aware that, by itself, interaction as such is not harmful. The problem is vulnerability $V_{t^m}(a_n)$ of an asset, where $V_{t^m}(a_n) \in [0,1]$. Only after adding this factor to the above equation, an appropriate risk value can be obtained as follows: $R(a_n,t_m) = v(a_n) * E_{a^n}(t_m) * V_{t^m}(a_n)$.

However, in the literature the first equation appears almost exclusively. So it is important to know that stating only $E_{a^n}(t_m)$ actually stands for $E_{a^n}(t_m) * V_{t^m}(a_n)$. Now, based on the values for $R(a_n,t_m)$, risks are prioritized and countermeasures are taken. Some additional discussion on this classical approach can be found in [3].

But the real problem is how to decide about an investment in counter-measures. Knowing that a significant part of assets belongs to non-tangible assets, exact values for the above equations rarely make sense. Further, the quantity of assets and resources is usually so large that doing exact analysis is almost impossible.

A qualitative approach is therefore usually taken, in which assets are categorized into a certain number of descriptive classes. Also probabilities of threats are categorized into a certain number of descriptive classes. By using tables such as that below, risks are estimated and priorities are determined.

threat description	threat frequency	L		H	
	vulnerability level	L	H	L	H
asset value level	low	0	1	2	3
	medium	1	2	3	4
	high	2	3	4	5

In the above table, "L" stands for "Low" and "H" for "High". To determine risk, let us assume that the estimated threat frequency is "L", and the vulnerability level estimated to be "H". If the value of an asset is "high" then the risk is described with value "3".

Using a descriptive, qualitative approach significantly eases risk management processes. This is, so to say, a legitimate approach also according to accreditation standards like COBIT and ISO 17799 [1,7] (an interesting comparison of both methodologies can be found in [9]).

However, having risk management related data in the form of one large spreadsheet is a poor basis for grasping the risk situation. Such a presentation is not easily perceived by humans and the whole logic, the complete process and the relationships that are the basis of risk management, are lost. Thus a new approach needs to be developed that provides a holistic view on risk management, presents its dynamics, all key elements and their relationships, together with the big picture of risk management, in appropriate graphical form. A picture is worth a thousand words.

3. The New System Dynamics Based Approach to Risk Management

System dynamics was developed by Jay Forrester in the early sixties and is now an established discipline [2]. There already exist some attempts to use system dynamics for improving information systems security, e.g. [4,5]. Using system dynamics with a focus on risk management has been suggested in [8], and this is the basis for the research presented in this paper.

One central idea of system dynamics is causal loops (or feedback loops) that are formed by setting causal links, i.e. relations between variables. A positive link polarity means that increasing a

driving variable increases the driven variable, and vice versa. Variables can be material or non-material (e.g. beliefs). Further, they can be stocks, rates and constants.
These qualitative diagrams are intuitive and expressive, and provide an insight into systems structure and functioning. Further, they serve as a basis for quantitative models, when backed by formulae that quantify variables and their relationships.

Fig. 1 demonstrates a generic risk management model for information systems. The basic variables are asset value (AV), threat probability (TP), risk (R), safeguards investments (SI), current asset vulnerability (CAV), and months of exposure period (MOE). These variables form two balancing loops that are powered by threats through threat probability - R, SI, MOE and R, SI, CAV are these two balancing loops.

Threats are generators in the background of each and every risk management process and their treatment is based on their probabilities. In our case this probability states the likelihood that a threat interacts with a particular resource during a certain one-month period.

There are additional variables that serve for proper dimensioning, scaling, and translation, i.e. for tuning the model to a concrete environment. These variables include amortization rate (AR), initial asset vulnerability (IAV), default exposure value (DEV), compensation factor (CF), vulnerability neutralization value (VNV), exposure compensation trigger (ECT), acceptable risk value (ARV) and delay (D).

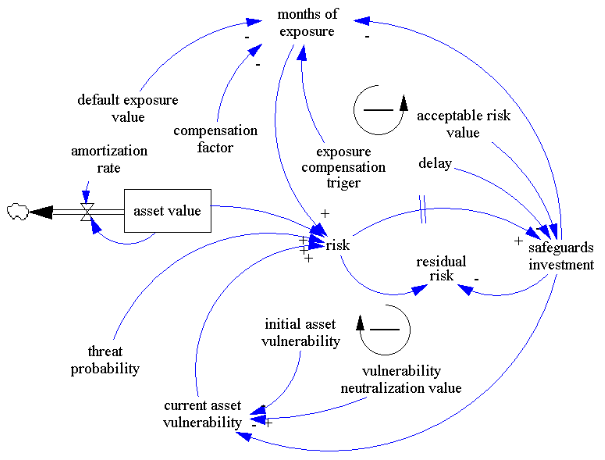

Figure 1: Causal loop diagram of risk management

Delay denotes the time between the point when risk becomes constituted and that when safeguards are implemented. It is also assumed that this is the only delay in the whole system that influences safeguard investments. But usually the implementation of countermeasures is also delayed due to human factor perception and by organizational issues. Further, ECT serves to include or exclude exposure as a risk driving variable. The roles of other variables should be clear on the basis of their names.

Last but not least, there is one important fact that is also explicitly presented in our generic model. This is residual risk (RR). Very often, risk cannot be completely eliminated, or some risk may be intentionally taken into account, and this is what residual risk is about.

4. Simulations

In order to demonstrate an application of this model, only two basic simulations will be presented due to limited space. Both are taking 24 months with simulation increment being set to 0.03125 month.

The initial value of an asset is 100, while initial values of other variables are as follows: DEV = VNV = D = 0, AV = ARV = TP = 0.1, and CF = IAV = 1. The simulation results of this basic set up are given in Fig. 2. It can be seen that variables AV, RI, SI and CAV exhibit expected behavior, which is dictated by a naturally diminishing value (amortization) of the asset, assumed to be 10% per month.

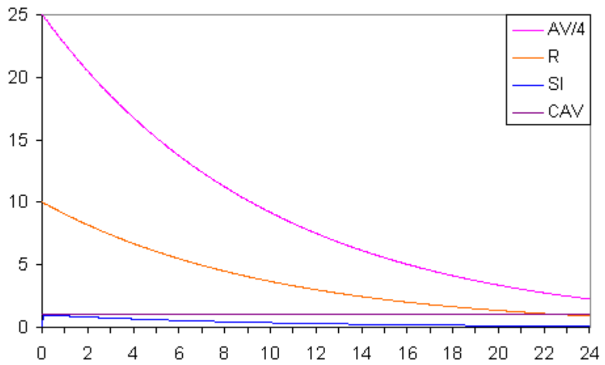

Fig. 2: Results of the first simulation run with (x-axis presents months, AV is scaled for clarity)

Now changing only two variables, TP from 0.1 to 0.5 and VNV from 0 to 0.2, one very interesting property appears. R, SI and CAV start to oscillate (see Fig. 3).

By enlarging D, oscillations preserve their amplitude, but their period is enlarged. This helps to identify the main source behind these oscillations – in this case, the very delay between observed risk and reactions, i.e. investments and consequently implementation of the necessary safeguards. It is interesting to note that, by including months of exposure, change in threat probability again leads to oscillations without changing VNV.

These facts provide the basis for a more detailed study and for improving decision making processes with regard to risk management. Future work should certainly also address another loop that appears in reality, which links SI and TP. This latter one is very hard to address but, for completeness of the problem, this task has to be done. And finally, human perception has to be included in the model.

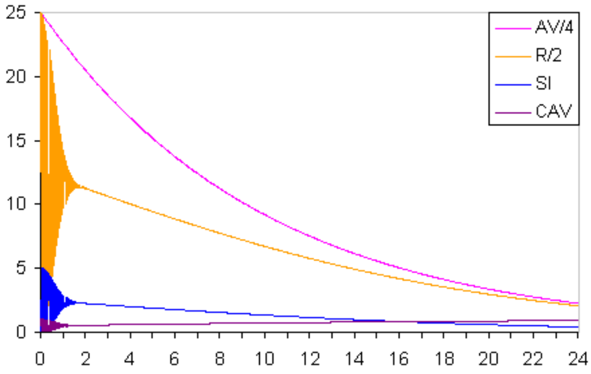

Fig. 3: Results of the second simulation run (R and AV are scaled because of clarity)

5. Conclusions

Risk management is at the heart of information systems security. But due to increasing complexity of information systems (intensive networking, numerous existing and emerging services, and exponentially increasing data that present one of the core assets of each organization), traditional techniques are no longer sufficient. There are many disadvantages of those techniques, some of the most important being lack of visibility of relationships between all related elements (i.e. lack of holistic graphical causal presentation), and lack of visible dynamics. Traditional techniques are not really suitable for simulations to anticipate future trends as well. This limits their use to improve decision making for information systems security.

To overcome these problems, a new generic risk management model has been developed that clearly identifies information systems security related elements and their relationships. It further enables quantitative treatment, together with simulations, by use of system dynamics.

It has been demonstrated in this paper how this model can provide useful insights into risk management dynamics. And being integrated properly into existing information systems and tied to threats through e.g. automatic data exchange about threats with relevant sources like CERTs, a real time decision supporting environment can be build to improve security related decision making.

References:

[1] COBIT Steering Committee, *COBIT Overview*, Information Systems Audit and Control Foundation, Rolling Meadows, 1998.

[2] Forrester J., *Industrial Dynamics. MIT Press*, Cambridge, 1961.

[3] Gerber M., Von Solms R., Management of risk in the information age, *Computers & Security*, Vol. 24, No. 1, 2005, pp. 16-30.

[4] Gonzalez J.J., Sawicka A., A Framework for Human Factors in Information Security, *Proceedings of the WSEAS Conference on Security, HW/SW Codesign, E-Commerce and Computer Networks*, Rio de Janeiro, 2002.

[5] Gonzalez J.J. (editor), *From Modeling to Managing Security - A System Dynamics Approach*, Höyskole Forlaget AS, Kristiansand, 2003.

[6] International Standards Organization, *Information Processing Systems - Open Systems Interconnection - Basic Reference Model, Security Architecture, part 2*, ISO Standard 7498-2, Geneva, 1989.

[7] International Standards Organization, *IT - Code of Practice for Information Security Management*, ISO 17799, Geneva, 2000.

[8] Trček, D., *Managing information systems security and privacy*, Springer, Heidelberg / New York, 2006.

[9] Von Solms B., Information Security governance: COBIT or ISO 17799 or both? *Computers & Security,* Vol. 24, No. 2, 2005, pp. 99-104.