This is an early version of the paper "Trček D., System Dynamics Based Risk Management for Distributed Information Systems, Proceedings of ICONS 09, IARIA / IEEE, Gosier, 2009" with figures being intentionally distorted (due to IPR issues & public dissemination).

System Dynamics Based Risk Management Model for Distributed Information Systems

Denis Trček[1]

Abstract: Networked information systems have not been restricted to closed organizations environments for more than a decade. They are now crucial in supporting operations of infrastructure, ranging from power plants to air-control systems. These networked information systems, essentially forming the current internet, are thus highly sensitive kinds of infrastructure where security plays a central role. However, assuring their security has to address certain specific aspects with regard to risk management. This paper presents a new approach and a generic risk management model for distributed information systems that deploys system dynamics. Such an approach provides many advantages, like suitability for interdisciplinary use, providing a graphical view on the system structure and components relationships, real-time support for "what-if" scenarios, and the possibility for inclusion in automated decision support systems. It is especially suitable for education and risk awareness programs in organizations.

Keywords: information systems security, risk management, risk perception, system dynamics, simulations, decision support.

* Laboratory of E-media, Faculty of Computer and Information Science, University of Ljubljana, Tržaška c. 25, 1000 Ljubljana,, Slovenia.

e-mail: denis.trcek@fri.uni-lj.si

1. Introduction

Security in information systems (IS) is becoming a well-established discipline, where each and every security related activity has to start with the basics. These constitute risk management.

Although risk management research and its application have long and proven record, their application to information systems is not straightforward because of the specifics of contemporary information systems. Current networked information systems belong to one of the most complex systems of human creation and have penetrated all segments of our life. According to Internet Systems Consortium, the number of hosts in the internet in July 2006 was 439,286,364 (Internet Systems Consortium, 2006). Further, a typical host that runs, for example, MS Windows operating system, has a few thousand COM (Component Object Model) elements. Further, even on local operating systems, the number of interactions between these components exceeds practical possibility of addressing all security issues. In addition, a growing number of these components are becoming mobile, which means that their place of origin differs from the place of execution. On top of this, there is a human factor that interacts with these systems, not to mention interactions between humans themselves. It is evident that there are “endless” possible interactions in globally networked, distributed information systems. To make things even worse, a dominant proportion of the assets belong to non-tangible assets. This makes security-related treatment, i.e. risk management, quite specific.

In many cases, when managing risks in information systems, we are left with qualitative methodologies. Of course, quantitative methods remain a priority on our wish list. This is elaborated in more detail in the second section. In the third section, system dynamics is shortly introduced and its suitability for risk management in information systems is evaluated. A new methodological approach is taken with layering system dynamics models in a way that is known in the engineering world. This approach enables the above-mentioned elements to be addressed more effectively to improve decision making in information systems security. Using this approach a generic model for risk management in IS is presented in the fourth section. In the fifth section simulations of this model are given and analyzed. There is a conclusion in the sixth section, followed by references. In the appendix, there is the complete listing of the simulation model.

2. Specifics of Risk Management Methodologies for IS

The necessary definitions of elements and relations that form risk management and that are based on the relevant standards (ISO, 2004) are given first.

At the core of risk management there are assets and threats. Assets are defined as anything of value to an organization, while threats denote any potential cause of an incident. Risk, which means the potential of a given threat to exploit vulnerabilities of an asset and cause damage, emerges as a consequence of interaction between assets and threats.

In order to minimize risks, risk analysis takes place, which means identifying security risks, their magnitude and required safeguards. In the case of IS, safeguards comprise practices, procedures or mechanisms that reduce risks. This risk minimization process results in residual risk, which means the risk remaining after the implementation of safeguards.

Risk management in IS, which means the total process of identifying, controlling and minimizing (or eventually eliminating) events that may endanger resources, is embodied in security policy. Logically, how much risk an organization is willing to take is a matter of security policy.

The most basic approach to risk management starts with a set of assets $A = \{a_1, a_2, ..., a_n\}$ and a set of threats $T = \{t_1, t_2, ..., t_m\}$ to form a Cartesian product 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 a probability $E_{a_n}(t_m)$ of interaction with this asset during a certain period is determined. Interaction as such is not harmful. The problem is vulnerability $V_{t_m}(a_n)$ of an asset, where $V_{t_m}(a_n) \in [0,1]$. After taking this into account, an appropriate risk estimate can be obtained: $R(a_n,t_m) = v(a_n) * E_{a_n}(t_m) * V_{t_m}(a_n)$.

Besides this basic quantitative approach, other quantitative methodologies can be applied. In (Ryan and Ryan, 2005) nonparametric methods are given as a basis for analysis of failure times in order to derive probability distributions of systems failures (these failures are the consequence of successful breaches of security services). This basis is improved by correlating system survival times to the use of certain design enhancements and other threats countermeasures. In (Andrijcic and Horowitz, 2006) a specific risk analysis is presented for the field intellectual property rights.

But the real problem with every quantitative methodology for risk management in information systems is that a significant part of the assets of organizations belong to non-tangible assets, e.g. data and goodwill, as discussed in (Gerber M., Von Solms R., 2005). How to identify and value all the data that range from e-mails to system logs? To make things even worse, the most important assets are employees. Due to the specifics of these kinds of assets, they are hard to value (none of these assets is recorded and valued in balance sheets). And finally, whatever the asset and related threat, getting exact values for its vulnerability and threat probability exceeds our capabilities due to the number of resources in IS and related threats. What is most feasible, is an approach on the aggregates level.

Taking all this into account, a qualitative approach is often taken. Assets are categorized into a certain number of descriptive classes, which also holds true for threats and vulnerabilities. By using tables such as that below, risks are estimated and priorities are determined. For example, let estimated threat frequency be low and estimated vulnerability level high. When the value of an asset is "high" then the risk is described with value "3".

threat	threat frequency	low (L)		high (H)	
	vulnerability level	L	H	L	H
asset value level	marginal	0	0	1	1
	low	0	1	2	3
	medium	2	3	4	5
	high	4	5	6	7
	extreme	6	7	8	9

Table 1: Risk management in information systems – a possible qualitative approach

Using a descriptive, qualitative approach significantly eases risk management processes. This is a legitimate approach also according to standards like (COBIT, 1998) and (ISO, 2000).

However, the qualitative risk management approach also has significant drawbacks. As stated in (Cox, Babayev and Huber, 2005), these approaches suffer from the following two important weaknesses:

- reversed rankings, i.e. assigning higher qualitative risk ratings to situations that have lower quantitative risks;
- uninformative ratings, i.e. frequently assigning the most severe qualitative risk label (such as "high") to situations with arbitrarily small quantitative risks and assigning the same ratings to risks that differ by many orders of magnitude.

As a consequence, the value of information that qualitative approaches provide for improving decision making can be zero in the case of many small risks and a few large ones, where qualitative ratings often do not distinguish the large risks from the small. This further justifies the fact that quantitative treatment has always to be the preferred option.

3. System Dynamics

IS security is an area defined by technology and the human factor and assuring security in such area is not easy. What is evident is that general and elegant analytical risk management solutions will probably be the exception. We will be left mainly with computer simulations. Summing up all the specifics given so far, the requirements for applicable methodologies are as follows (Trcek, 2006):

1. First, these methodologies should support modeling of information systems' core characteristics. This includes complexity, where interplay between humans and technology is governed by numerous feedback loops. Further, these systems are mainly non-linear and highly dynamic.
2. Secondly, the methodologies should enable multidisciplinary and / or interdisciplinary research, including IT, management, psychology, and sociology. As a consequence, they should be intuitive, because experts from various domains with diverse professional cultures will have to cooperate. Therefore these methodologies should enable effective representation and communication about phenomena that are the subject of research in IS security.

3. Thirdly, humans do not easily perceive plain numerical presentation and the whole logic, the complete process and the relationships that are behind risk management in information systems, becomes blurred with such a presentation. A holistic view of risk management, the big picture of risk management, needs appropriate graphical support.
4. Fourthly, although qualitative models have scientific merit, support for quantitative modeling from required methodologies remains a priority where possible.
5. And fifthly, due to the specifics of information systems resources stated above, an approach on the aggregates level should be supported.

A methodology that meets the above requirements is system dynamics - Jay Forrester developed it in the early sixties (Forrester, 1961). Some attempts already exist to use system dynamics for improving information systems security, e.g. (Gonzalez and Sawicka, 2002) and (Gonzalez, 2003). Using system dynamics with a focus on risk management has been suggested in (Trcek, 2005), and this is the basis for the research presented in this paper.

The central idea of system dynamics is diagrams, composed of causal loops, or feedback loops, which can be positive (reinforcing) and negative (balancing, stabilizing). Setting causal links, i.e. relations, between identified variables, forms these diagrams. Where a link has positive polarity this 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 provide an insight into systems structure and functioning. They serve as a basis for quantitative models, when backed by formulae that quantify variables and their relationships.

System dynamics is based on the premise that all kinds of behavior, including chaotic ones, emerge from the following basic building blocks:

- exponential growth - this is a consequence of a positive feedback loop;
- a goal seeking pattern - this is a consequence of a negative feedback loop;

- oscillation – this arises where a goal seeking pattern has time delays in the negative loop;
- S-shaped growth - this arises from interaction of a positive feedback loop that prevails at the beginning, then becomes dominated and stabilized by a negative feedback loop;
- S-shaped growth with overshoot – this is derived from S-shaped growth, but delays take place in the negative feedback loop;
- overshoot and collapse – this is derived from S-shaped growth structure with an additional negative feedback loop that drives the system back towards initial conditions, and away from the stabilization point of S-shaped growth.

These are, so to say, the atomic building blocks of system dynamics. Using these basic structures, causal feed-back loop diagrams are obtained that model real-life phenomena.

An important point that is related to interdisciplinary issues of research in this field has to be addressed here. Management science is often dealing with complex systems - systems where human factor is involved can be almost automatically characterized this way. In these areas, pure analytical solutions are mostly out of our reach. But due to increasingly available computing power, quantitative approaches, based on computer simulations, can be used. They could complement most commonly used case-studies approaches, which used to be the most frequently used approach to deal with complex systems. But the problem is that case-studies serve to analyze typical phenomena on a case by case basis.

In engineering, the approach is often different. Some basic building blocks are used to form a new, higher level construct, and so on until the final implementation is done. For example, in the software industry, the very basic building blocks are software languages with data types and procedures that present the starting point. The next level aggregates are objects, where general-purpose procedures and data are narrowed for a more specific use, i.e. to perform certain elementary tasks. At the next level, objects are grouped into components and, at the final level, where the actual implementation of the final technical solution takes place, appropriate components are selected and orchestrated accordingly to achieve the final service. Similar approaches can be also found in other areas of engineering like electronics.

Therefore in systems dynamics, conceptually, a gap exists between basic building blocks and majority of final models - this is also the case for security in information systems. Taking into account the fact that deployment of system dynamics for security in information systems is still at its early stages, this is a good opportunity to base it on a layered, modular approach. Such an approach is expected to improve flexibility and usability. One important note – this is not to say that system dynamics has no "second level" constructs. There are some such constructs, e.g. the Bass diffusion model for innovations that overcome the startup problem. But the point is to build systematically such second level blocks for security in information systems.

The procedure in this paper therefore follows the following steps:

1. Using the basic building blocks, the first level model (layer 1 model) is built that presents the core variables and their relationships graphically. This qualitative model generally addresses a particular area of application at the level of conceptual understanding.
2. In the next step, supporting variables for scaling and translating are included that enable tuning of the former model to a concrete environment. Additional variables are also needed for dimensional consistency. This results in the layer 2 model that is already suitable for the range of environments that face the particular problem area. Further, the layer 2 model identifies potential variables and their relationships that need further experimental elaboration.
3. In the third step, particular functions are defined for the model. Concrete inputs with intervals and increments for all the variables are introduced. If some final variables are needed for dimensional consistency, these are also introduced. This phase results in the fully applicable, layer 3 model, which is ready to support qualitatively and quantitatively decision-making processes for a specific area and a particular case.

4. The Generic Model

Figure 1 presents the layer 1 model of the generic system dynamic based model for risk management in information systems. From the human resources point of view, the core variables are risk (R) and risk awareness (RA). Risk awareness is directly related to safeguards investment (SI). As a consequence, residual risk (RR) is driven by the difference between R and SI. SI can follow three paths for neutralization of R. The first includes reduction of the exposure period (EP), which is the period of assets to be effectively confronted with threats. The second path includes reduction of current threat probability (CTP), which covers actions directly related to neutralization of threats. The third path includes reduction of current asset vulnerability (CAV), which covers activities for improving resistance of assets.

The whole risk management process is carried out to protect an asset that has a certain value (AV). AV is continuously diminished through amortization, according to the amortization rate (AR). Note that AV is an accumulator, as well as RA. The difference, however, is that AV is a material level, while RA models a state of mind, which is related to information delay. The perceived value is getting adapted on the basis of reported value and mental inhibitors that dictate the process of adaptation.

The complete model consists of three balancing loops, which are (R, RA, SI, EP), (R, RI, CTP) and (R, SI, CAV). Taking into account that there is no explicit reinforcing loop, "a generator" seems to be missing. But its role is being played by a threat, more precisely by CTP.

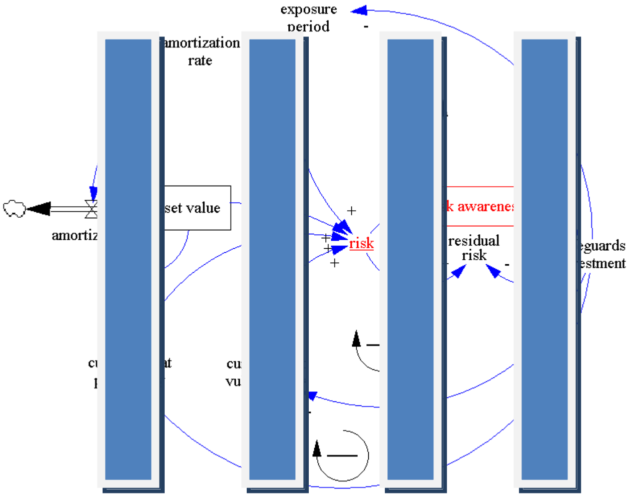

Figure 1: Causal loops diagram of risk management - layer 1

This layer 1 model is the core model for understanding the whole point of the paper. In order to adapt it for simulations, it has to be further elaborated to the layer 2 model (see Fig. 2). This model includes a default exposure value (DEV) and an exposure neutralization value (ENV). The role of the first parameter should be clear, while the second parameter serves to support tuning to a particular environment. The exposure compensation trigger (ECT) is a switch that enables exclusion of the EP feed-back loop for easier debugging.

The same logic that is behind DEV and ENV is also behind initial threat probability (ITP) and probability neutralization value (PNV), and behind initial asset vulnerability (IAV) and vulnerability neutralization value (VNV). With regard to RA, mental adjustment time is a constant that is often used in modeling mental adaptation processes, e.g. exponential smoothing (Makridakis et al., 1983). In addition, two delays are explicitly drawn: from R to RW, and from RW to SI. The first is required by the very nature of stocks (and flows), while the second denotes the fact that there always exists a delay between changed perception, i.e. *RA, and reaction, i.e. SI. For example, some orders have to be executed, funds allocated, etc.*

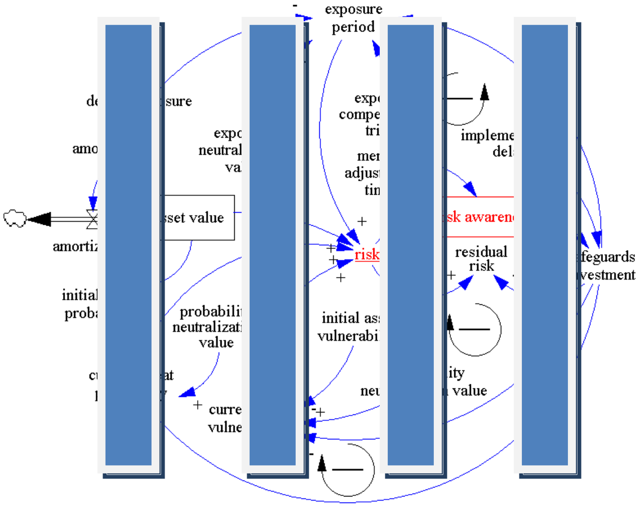

Figure 2: Causal loops diagram of risk management – layer 2

Layer 3 model in our example has the same structure as that given in Fig. 2 and does not need further elaboration. However, to be fully defined, it needs quantitative values and functions between variables, so the complete listing is given in the appendix.

5. Simulations and Discussion

This section presents simulations done with the model described in the previous section. A typical tangible resource is assumed, e.g. a PC, which has an amortization period of two years, and amortization rate of ten percents per month. The use of non-tangible asset is straightforward – an appropriate custom design function has to be defined to reflect the time specifics of such resource. All simulations take 24 months, with simulation increment being set to 0.03125 month, and with graphs presenting the core variables, which are R, RA, SI. For easier explanation, RR is also included. On all graphs, *x*-axis presents months, while units for all the variables are found in the listing in the appendix.

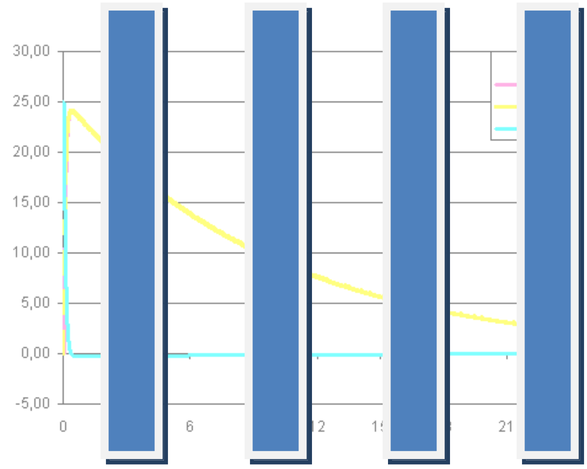

Fig. 3: Results of the initial simulation run

The initial value of an asset is 100 monetary units, while initial values of other variables are as follows: DEV = ENV = 1, ECT = ID = VNV = PNV = 0, ITP = IAV = 0.5 and MAT = AR = 0.1.

The simulation results of this basic set up are given in Fig. 3.

Now suppose that MAT is increased to e.g. 0.9. Consequently, this enlarged delay results in negative RR, because of over-investment in safeguards (see SI). To make this situation more visible, AR is also increased to 0.3 (see Fig. 4).

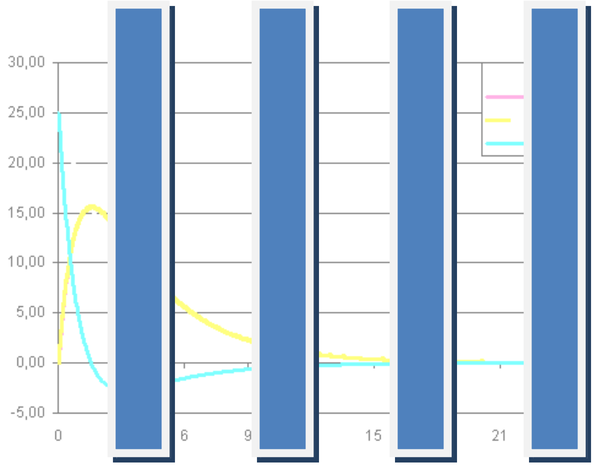

Fig. 4: Results of the second simulation run

Now suppose we additionally include an implementation delay and set ID to 5. The over-investment in SI becomes even more visible, as shown in Fig. 5.

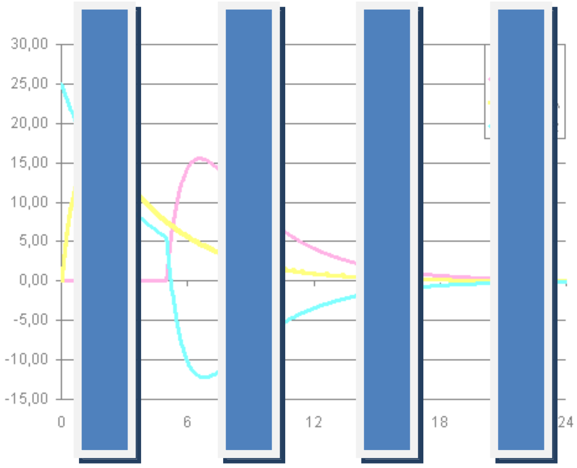

Fig. 5: Results of the third simulation run

The above situations suggest that the system may be subject to oscillations. Starting again with initial setting and enlarging PNV and VNV to 2, reveals small, but visible short oscillations of CTP and CAV (and consequently R). The only reason can be MAT, and increasing MAT from 0.1 to 0.8 indeed damps oscillations (see Fig. 6 with MAT = 0.1). This means that the system is sensitive to quick mental changes.

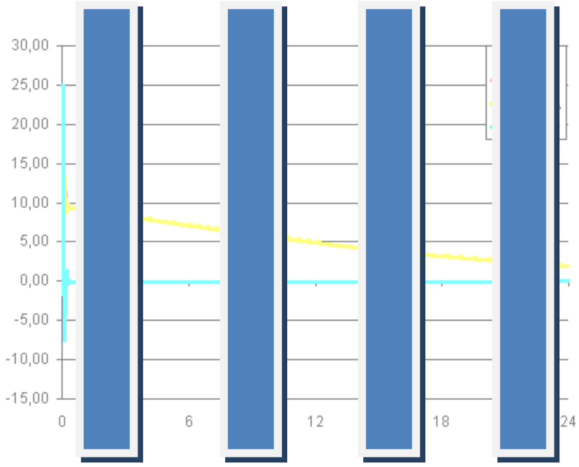

Fig. 6: Results of the fourth simulation run

But oscillations still remain hidden in the system, which can be assumed on the basis of the first four simulation runs. It is anticipated that by enlarging ID, oscillations should appear again. And this indeed turns out to be true, as shown in Fig. 7, where ID is set to 2.

Until now, the upper casual loop that includes EP has been excluded. Including this feed-back loop results in patterns where regular shapes are starting to disappear. In this particular case, where we are entering the "chaotic" regime, DEV was set to 15 (see Fig. 8).

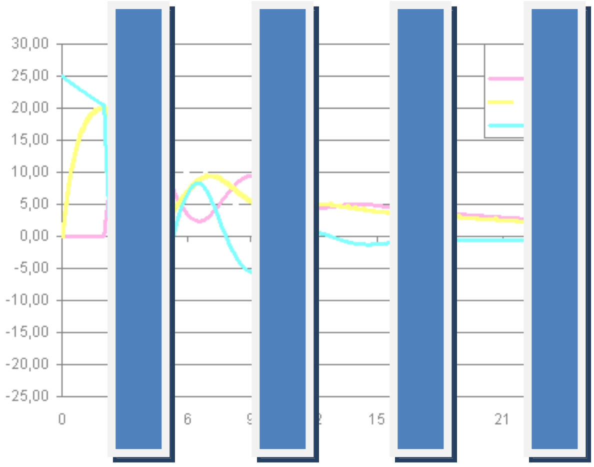

Fig. 7: Results of the fifth simulation run

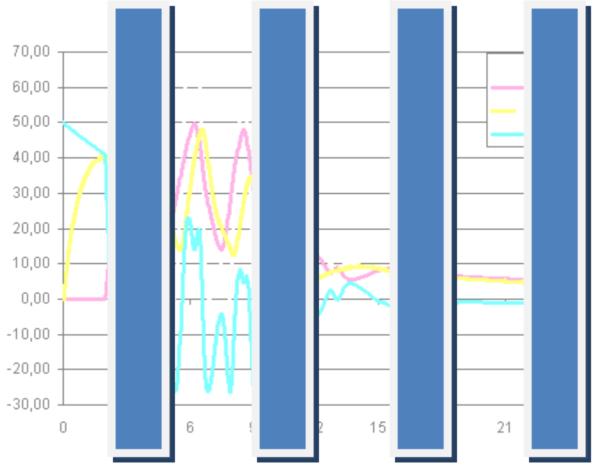

Fig. 8: Results of the sixth simulation run

In reality, all feed-back loops are simultaneously present. Therefore the decision-making process for risk management in information systems can be well supported with system dynamics and generic models like the one presented here. Such models enable bottom-up building of knowledge about the system and familiarity with the final situation that is "chaotic". Put another way, being faced with patterns that are close to chaotic behavior scarcely gives clue as how to react efficiently and what this pattern is really a result of..

6. Conclusions

We are witnessing strong penetration of networked information systems in all areas of our lives. Their security is thus of utmost importance. Risk management is at the heart of information systems security. But due to the increasing complexity of information systems (intensive networking, numerous existing and emerging services, exponentially increasing amounts of data, strong involvement of human factor, an almost countless number of possible interactions), traditional techniques are no longer sufficient. As quantitative methods are preferred, it turns out that dealing with risks in an analytical way becomes almost impossible. Exact analytical solutions are just an exception, while quantitative treatment remains a feasible option if computer simulations are chosen. This gives additional advantages that traditional quantitative approaches lack; they often lack visibility of relationships between involved elements (i.e. lack of holistic graphical causal presentation), and barely captures the dynamics of a system. Another problem is their suitability for simulations to efficiently anticipate future trends. This limits their use to improve decision making for information systems security.

To overcome these problems, system dynamics has been used and 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 built to improve security related decision making. The model is already suitable (and already used) in education and security awareness programs.

7. References

Andrijcic E., Horowitz B., A., (2006). A Macro-Economic Framework for Evaluation of Cyber Security Risks Related to Protection of Intellectual Property. *Risk Analysis*, 26(4), p. 907, 2006.

COBIT, (1998). *COBIT Overview.* Information Systems Audit and Control Foundation, Rolling Meadows.

Cox, L.A., Babayev D., Huber W., (2005). Some Limitations of Qualitative Risk Rating Systems. *Risk Analysis*, 25(3), p. 651.

Forrester J., (1961). *Industrial Dynamics.* MIT Press, Cambridge.

Gerber M., Von Solms R., (2005). Management of risk in the information age, *Computers & Security*, 24(1), pp. 16-30.

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

Gonzalez J.J., Sawicka A.., (2002). 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.

International Standards Organization, (2000). *IT - Code of Practice for Information Security Management*. ISO 17799, Geneva.

International Standards Organization, (2004). *IT - Management of Information and Communications Technology Security, Part 1: Concepts and Models for Information and Communications Technology Security Management*. ISO / IEC standard 13335-1, Geneva.

Internet Systems Consortium, (2006). *ICS Domain Survey: Number of Internet Hosts*. http://www.isc.org/index.pl?/ops/ds/host-count-history.php

Makridakis, S., Ersen, A., Carbone, R., Fildes, R., Hibon, M., Lewandowski, R., Newton, J., Parze N. E., Winkler, R., (1984). *The Forecasting Accuracy Of Major Time Series Methods*. New York, John Wiley & Sons.

Ryan J.J.C.H., Ryan D.J., (2005). Proportional Hazards in Information Security. *Risk Analysis*, 25(1), p. 141.

Trcek D., (2005). *Managing information systems security and privacy*, Springer, Heidelberg / New York.

Trcek D., (2006). Security Models: Refocusing on the Human Factor. *IEEE Computer*, 39(11), pp. 103-104.