Information Systems Security Management By Deployment of Innovations Management Techniques

Denis Trček
Faculty of computer and information science
University of Ljubljana
Tržaška c. 25
1000 Ljubljana, SLOVENIA
denis.trcek@fri.uni-lj.si http://fri.uni-lj.si/

and

Borut Likar
Faculty of management
University of Primorska
Cankarjeva c. 5
6000 Koper, SLOVENIA
borut.likar1@guest.arnes.si http://fm.upr.si/

Abstract: Information systems security is one the hottest topics in the era of global competition, not only at organizations level, but also at states level. The situation is getting even more complicated because of advancements in the area of information technologies (IT) because we now have to deal with almost amorphous information systems (IS) due to their integration with ubiquitous computing devices on one hand and transition to cloud on the other. Nevertheless, organizations and states have to ensure security of such increasingly complex information systems despite this complexity. But dealing with the described situation exceeds potentials of standard approaches to information systems risk management and new approaches have to be developed, and adopted to neutralize newly emerging risks. This paper therefore presents an approach that is based on innovation management techniques and is focused not only on reactive and active risk management in contemporary information systems, but also (and primarily on) pro-active risk management.

Keywords: security, information systems, security policies, innovations methods.

1. Introduction

Nowadays, significant changes in the area of information systems (IS) are taking place – on one hand they are converging towards cloud computing, while on the other hand they are becoming extended by ubiquitous computing devices, also often called the Internet of Things that includes sensors, intelligent agents, RFIDs, etc.

Comparing now these newly emerging architectures with traditional architectures of information systems, which were geographically and administratively centered at organizations main premises, it is evident that we are facing a new, more complex structure, where administrative boundaries are changed in a way where the majority of administrative power is out of our hands, while geographical boundaries are often hard to identify. Clearly, traditional risk management methods that used to serve the purpose in the past are not sufficient anymore and have to be appropriately adjusted, extended or maybe even replaced.

To achieve this goal of appropriate handling of new IS architectures, this paper presents a method called Management Method for Integrative Information Systems Security, MIS^2 ("mee-square"), which is being developed now for approximately four years. To make its purpose and benefits more clear, this paper in the second section gives fundamentals of risk management related to information systems. In the third section basics of MIS^2 method are presented, while there are conclusions in the fourth section. The paper ends with acknowledgments and references.

2. IS Risk Management Basics

Each endeavor in IS security provisioning should be based on risk management procedure. The core of this procedure goes as follows [1]:

1. Identify your information systems assets and resources and their value.
2. Identify threats that exist in your environment and present harm potential for your assets.
3. Identify vulnerabilities of your assets in relation to the threats.
4. Make a prediction of how likely it is that a certain threat will exploit a certain asset in a given time frame (exposure period) – based on the value of your asset this gives you an expected loss in the given time frame, which means your risks.
5. Prioritize risks and start dealing with those most urgent ones. Risks elimination can be achieved by reducing the exposure of an asset to a threat, by reducing its vulnerability or reducing its value. This last option is the trickiest one, rarely applicable, but not impossible – one such case is, e.g., making multiple copies of certain data that a particular threat wants to delete, when these data are an asset in question (making numerous exact copies of large amount of data costs almost nothing, while the value of one deleted copy is thus negliable).

The above procedure can be nicely represented by a diagram that is given in Fig. 1.

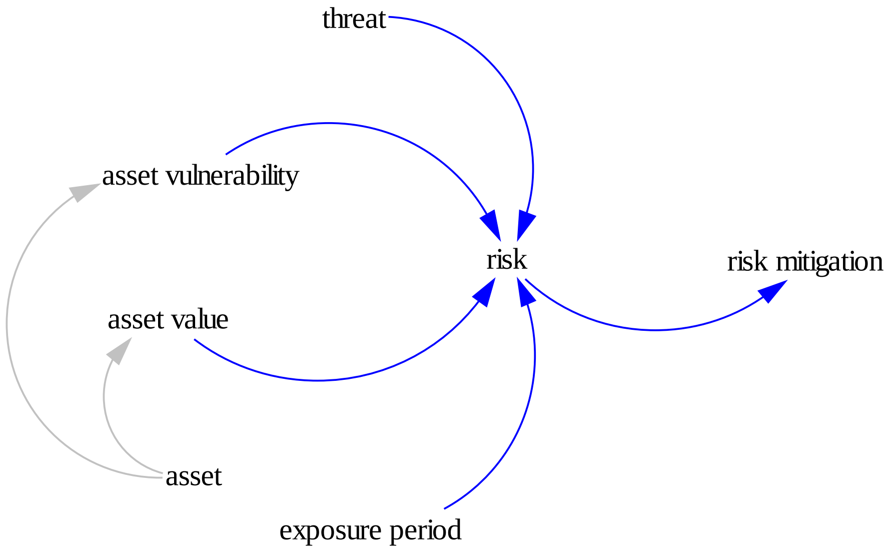

Figure 1: Risk management in IS – its elements and their relationships

Now as to risk management steps, the first step is quite straightforward – it is a matter of a systematic administrative procedure. The second step is not so trivial anymore – identifying threats already requires sufficient familiarity with IS technologies and concrete implementation details, not to mention managerial procedures. Similar holds true for the third step, which is in fact even harder than the second step. The same applies for the fourth step, while the fifth step is again a matter of a straightforward administrative procedure.

Actually, standards that exist in this area (the most notable representative being ISO 27000 family of standards [2]) do not provide any concrete guidance about steps 2, 3 and 4 in a sense as discussed above. Clearly, appropriate data should be used for this purpose, but the reality shows that these data rarely exist, so quantitative estimates are mere exception than a rule, and these procedures are mainly performed in a qualitative way.

Being faced with this limitations we have started to search for possible solutions already a few years ago and the first efforts of this research can be found in [3], with more details being given in the next section.

3. Management Method for Integrative Information Systems Security

Risk management has basically three epochs. The first one is concerned with past events and for these events, in principle, quantitative and qualitative data exist.

Risk management focused on this epoch is referred to as reactive risks management.

The second epoch is related to events that are taking place in current time. For this epoch quantitative and qualitative data in principle exist as well (however, obtaining quantitative data in many concrete cases remains an unrealistic option). Risk management for this epoch is referred to as active risk management.

The third epoch is about events that are expected to happen in the (near) future. Risk management concerned with this epoch is referred to as pro-active risk management.

Clearly, the hardest task is pro-active risk management. It can be supported by (data from) reactive and active risk management in a way as this is the case with ordinary forecasting methods like those used for, e.g., econometrics, technology forecasting. However, security of IS is a different story – standard forecasting methods make sense in cases where we deal with phenomena that have a strong, sufficiently long history (and stable in terms of statistical properties). Now in case of IS, radically new solutions may emerge, while traditional ones may be replaced sooner than sufficient data would exist to enable deployment of statistical methods.

This shows that dealing with IS risk management requires a different approach. One such solution is Management Method for Integrative Information Systems Security, MIS^2 [3]. The basic idea is to deploy creative thinking techniques for pro-active risk management by focusing on steps 2, 3, and 4 from the risk management procedure described in section 2. The MIS^2 method goes as follows:

1. Identification of MIS^2 participants: Within your organization identify first those employees that have sufficient knowledge about IT and those that are mere users and that are not particularly familiar with IT details.
2. Selection of MIS^2 participants: It is important to choose creative ones being able to think "out of the box". Therefore in the second step, partition the second population by filtering them on the basis of their innovative thinking potential. There exist methods how to do this and one such method can be found in [4].
3. Creative thinking session: Use the filtered part of the second population, which has sufficient innovative thinking potential, for being taught by security experts about generalities of IS security properties and functioning (avoid technical details to prevent mind-lock of these creative thinking individuals into particular existing solutions). Start a creative thinking session for risks identification and potential solutions with this group - deploy some of the established creative thinking methods like brainstorming (for more details a reader is referred to e.g., [5]) to identify IS risks and propose solutions.
4. Technical evaluation: To evaluate risks and proposed solutions, divide the population of IT specialists by using the same procedure as in the second step and filter out the most creatively thinking individuals that are familiar with IT details. It is useful to invite some participants from the group mentioned in step 2. Next, use these individuals to evaluate (in terms of technical feasibility) the results proposed by the first filtered group that was mentioned in step 3.
5. Financial and organizational evaluation: The results of evaluation in step 4 are given then to senior information security officers for economical feasibility evaluation and checking if they are aligned with strategic directions of the organization. It is important to focus on maximum three most serious threats at the same time.
6. Implementation: Implement the selected measures and periodically (regularly) repeat this procedures by systematically following its implementation to identify weaknesses and to further improve it.

It is worth to mention that we have already made some preliminary experiments with the proposed procedure and the results are encouraging [6]. Current experiments following the presented MIS^2 methodology have included two medium size private Slovene industrial enterprises with high value added to their products. These two experiments were followed by semi-structured interviews with CIOs and employees and some interesting results follow.

Generally speaking, in both enterprises CIOs had positive opinions about the MIS^2 method. The first CIO emphasized the inclusion of large number of non-IT specialized employees, where already the inclusion as such already had positive impacts and has increased awareness about importance of IS security. The second CIO has emphasized the advantage of providing new perspectives on IS security and that non-IT specialized have acquired new knowledge that is spread to other employees.

Further, it has turned out that both organizations were aware of quite some weaknesses, but many have still been unidentified until the experiment. When asked if they could estimate the opportunity costs of the most serious risk, the first CIO replied that this risk was related to access control in so called Enterprise Resource Planning (ERP) system. This system stored all the details of a sub-product that was completely developed and produced by their organization and then integrated into final products by many large European corporations. Without estimated consecutive costs, only acquiring details about this sub-product would be a serious issue that (in the pre-patent phase) could easily easy mean a damage of a few hundred thousands of EUR.

CIOs were also asked to state if the proposed method is representing an improvement to their IS security despite the fact that they already had formalized security policies. Both CIOs supported this proposition, and they planned to address newly identified risks in the next version of their organizations security policies, while the policy itself would be improved by including the principles of MIS^2 method. Moreover, the results would be used for the renewal of their ISO 27000 certification which was soon due.

4. Conclusions

It is interestingly to note that there are significant and important efforts going on in the area of quantitative risk management in IS – probably the most known such initiative is Making Security Measurable initiative being run by MITRE Corp. in the U.S. [7]. However, the problem areas and the proposed solutions that are addressed in this paper are not covered there and they can therefore present an important complement to this initiative.

In short, the quickly changing landscape of contemporary information systems puts additional requirements on provisioning of their security bet it at organizations or nations level. These changes are a consequence of newly emerging technologies, among which two most recent ones are cloud computing and ubiquitous computing. But our private, business and even state operations and functioning are increasingly depending on these systems. Therefore finding appropriate ways to deal with risk management in such IS in this situation is very important.

This paper therefore first gives the basics of risk management in IS. It identifies its steps and pinpoints those that are the most crucial ones. It further introduces three epochs of risk management, i.e. reactive, active and pro-active and shows the high importance of the latest one.

In order to provide appropriate tools for the most critical steps in pro-active risk management a method called MIS^2 (pronounced as “mee”-square) has been presented in this paper. It uses creative thinking methods used in innovations management. It is worth to mention that this method is already being tested in real environments, and some preliminary results are given in this paper.

We strongly believe that the method can present a valuable tool for (pro-active) risk management in advanced IS and its applications in real environments by the security community are encouraged to find out its weak points and to further improve it. Currently, this seems to be the only appropriate method (or approach) to risk management in advanced IS.

Acknowledgement

Authors acknowledge the support of the Slovene National Research Agency with the research program Pervasive computing P2-0359.

References:

[1] Trček D., *Managing Information Systems Security and Privacy*, Springer Verlag, Heidelberg / New York, 2006.

[2] International Standards Organization, Information Security Risk Management, *ISO/IEC standard no. 27005 (information systems security management standards family ISO 27000),* Geneva, 2008.

[3] Likar B., Trček D., A methodology for provision of sustainable information systems security, Cybernetics and Systems, vol. 43, no. 1, pp. 22-33, Francis & Taylor, 2012.

[4] Emma G.P., Inventions and the creative process, *IEEE Micro*, Vol. 25 , No. 3, pp. 96 – 95, IEEE, 2005.

[5] Likar B., Križaj D., Fatur P., *Innovations management*, 3. ed., Faculty of management, University of Primorska, Koper, 2012.

[6] Androjna A., Innovative Approaches to Pro-Active Information Systems Security Provisioning, M.Sc. Thesis, Faculty of management, University of Primorska, Koper, 2012.

[7] Martin R. A., Making Security Measurable and Manageable, *Proc. of the MILCOM 2008*, pp 1-9, San Diego, IEEE, 2008.