Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 43 (2015) 26 – 32

Procedia Computer Science

ICTE in Regional Development, December 2014, Valmiera, Latvia

CORAS for Threat and Risk Modeling in Social Networks

Aleksandrs Larionovs[a]*, Artis Teilans[a], Peter Grabusts[a]

[a]*Faculty of Engineering, Rezekne University of Applied Sciences, Atbrīvošanas aleja 90, Rēzekne, LV-4601, Latvia*

Abstract

As more users joining social networks possibility of threats is growing, as the information can be reached by expanding number of individuals that increases the possibility that the information „package" will find way to subjects with the appropriate degree of sensitivity to the information – vulnerability. Therefore, the risk management process and, in particular, the risk identification and analysis of key characteristics should be performed. Presented paper describes usage of CORAS methodology for modelling of social network risks.

Peer-review under responsibility of the Sociotechnical Systems Engineering Institute of Vidzeme University of Applied Sciences

Keywords: Social networks; Risk management and identification; CORAS.

1. Introduction

Social networks are online environment that attracts a wide range of interested people and users. Social networking comes with popularity, several structurally different sets of information and social networking are present; the increasing this popularity of Internet and its improved accessibility are already being discussed on scientific level. Addresses the people use in social networks and the threat that might happen could pose. Risk identification, research and solutions are essential to improve the socio-psychological space to prevent fraudulent and threatening activities that use social networks as a communication channel or use the information from these networks. Social networking is one of components there is necessary for a person's safety to determine the scope of the complex nature of human behaviour, actions, thinking forecasting, human impact is a complex process.

* Corresponding authors.
E-mail address: aleksandrslarionovs@inbox.lv; artis.teilans@ru.lv; peteris.grabusts@ru.lv

Peer-review under responsibility of the Sociotechnical Systems Engineering Institute of Vidzeme University of Applied Sciences
doi:10.1016/j.procs.2014.12.005

Social network users can be categorized by the different characteristics where one of the most important factors is the user's (profile owner's) age. Age is largely characterized user behaviour, the values reliance on information degree of psychological factors and attitudes towards the world around as a whole. Social networking is a key feature of the threat to information related to the management of the risks. Also risks cannot always be predicted and prevented because the formation of social networks is from people (at the different ages and with a great variety of individual characteristics) who can create, manage, and share information. A risk also is in social network as component of the information flow. That information complexity and low level of confidence in social networks makes it possible to carry out activities which can be seen as threatening in relation to a subject (user profile information space, geopolitical location, the Internet as a space in general).

Information speed in social networks takes place in a series of clusters – the threat of predictability and management complexity rises because information distributed by a single user to other users by certain amount of choice. Each of the recipients re-distribute or doesn't further disseminate that information. For qualitative changes in the future of social networking it is essential to find a solution to the indicators. With this indicators could be possible to manage the threat of social network information flow with high probability.

Social network structure can be described using an ontology-based approach, which is an important aspect of the threat classification. For example threat identification from network user's profile socio-psychological portrait (pre-school, primary school, teenagers, young adults online, seniors, considering age, gender and other criteria defined in the study). Traffic of information and related threats could be researched paying attention to the flow of the transition from one group of users to another group. It is important to research social network as information system with proper method.

2. Threats in information system - social network

Social networking is a key feature of the threat to information related to the management of the risks which cannot always be predicted and prevented because the formation of social networks is from people (at the different ages and with a great variety of individual characteristics) who desire to create, manage, and share information, be a component of the flow of information. That information complexity and low level of confidence in social networks makes it possible to carry out activities which can be seen as threatening in relation to a subject (user profile information space, geopolitical location, the Internet as a space in general).

Nature of research and analysis process of social networking contributes to system modeling and design situation, modeling, by promoting a competitive international scientists to be able to introduce the latest scientific knowledge of modeling socio-technical systems, making an opportunity for threat prediction, filing and describing the applicability of socio-economic and technical space. Social network is specific environment to risk mitigation measures.

Theories around technology and information technology have described various existing risks, some of which are as follows: contractual, economic, environmental, political, legal and security risks. During analysis special attention should be paid to the standard ISO 31000 (Risk management – Principles and guidelines[1]) described definitions of risk, which consists of five information systems inherent risk characteristics:

- Result or the deviation from the expected – positive and / or negative;
- Objects can have different aspects (such as financial, health and safety, environment), and they can be applied at different levels (such as strategic, organization, project, product and process);
- Risk is often characterized by reference to potential events and consequences or their combinations;
- Risk is often expressed as a combination of the effects of the events (including changes in circumstances) and it is related to the probability of the risk occurring;
- Uncertainty is the risk situation, even partial, resulting from deficiency of information related to understanding or knowledge of the event, its consequences or opportunities[1].

Modern information systems are exposed to various threats. The potential risk awareness of the circumstances and response is part of risk management. Risk management is a holistic process, which consists of several interrelated components.

Table 1. The risk management process components[2].

Source	Description
A Guide to the Project Management Body of Knowledge	Risk management planning, risk identification, qualitative and quantitative risk analysis, risk response planning and risk monitoring and control
A Guidebook of Project & Program Management for Enterprise Innovation	Risk management policy definition, risk identification, risk analysis and assessment plan for the risks preparation, execution plan for the risks and testing and monitoring
Tasmanian Government Project Management Guidelines	Project environmental assessment, risk identification, risk analysis, risk assessment, risk mitigation and risk monitoring and control, as well as of communication and consultation (consultation)
A Risk Management Standard	Organization's strategic objectives in relation to the evaluation of risk management, risk assessment, risk analysis (hazard identification, risk characterization, risk for evaluation), risk assessment, risk reporting, decision making, risk handling, reporting on residual risk, the risk management process as well as monitoring and changes to

Often risk management processes are such as the identification of new risks stating which could be repeated in other related processes. Table 1 contains information on a number of risk management processes. Risk management occurs at certain methodologies that can be used both individually and also combined. Best practice uses four risk management methodologies:

- Risk Management Guide for DOD Acquisition.
- A Risk Management Standard.
- Project Risk Management Handbook. Threats and Opportunities.
- Handbook for Integrating Risk Analysis in the Economic Analysis of Projects[3,4].

Risk Management Guide for DOD Acquisition. The Handbook of risk and risk management description and definition of terms is assessed to the risk management concept DoD acquisition processes, risk management is carried out, including Planning (Planning), assessment (Assessment), management (Handling) and monitoring (Monitoring).

The manual emphasizes that risk management is a structured (Disciplined), purposeful (Looking Forward) and continuous (Continuous), it is a planned and systematic (Planned Procedures), the future potential problems have been assessed (Considered) (Prospective Assessment) attention is paid to technical risks (attention to Technical risk), all risk management activities (All Aspects) documented, as well as the risk assessment carried out throughout the acquisition process cycle management activities assessed and if necessary modified, critical risks are constantly monitored (Continual process).

Authors of A Risk Management Standard define a standard goal and describe why it is necessary for standard and determine that it is necessary to agree on terminology, and emphasizes that the standard is summarized by best practices (Represent Best Practise). The standard is described in the risk management process and organization and risk management objectives. Also there are risks and risk management is carried out, definitions of terms and risk categories described in the risk management process, risk management process and risk policy.

Project Risk Management Handbook. Threats and Opportunities describe California’s DOT's risk management, including threats and opportunities (Both Threats and Opportunities) and its aim is to describe the project risk management planning and implementation processes and foundations. Handbook is intended for project managers, department, functional managers and other staff who are involved in the projects.

Handbook for Integrating Risk Analysis in the Economic Analysis of Projects. "Handbook for Integrating Risk Analysis in the Economic Analysis of Projects" publisher is the Asian Development Bank (Asian Development Bank). The manual is included for assessment of risk analysis experience, risk analysis theory and a variety of risk analysis methods.

In conclusion, the various approach of risk management are not having principle differences on the process. The difference is on the level of detail and context of risk management assessment. On the other hand, more detailed analysis and description of the risk management can be divided into two major aspects: the risk monitoring and risk response.

3. Risk management methodology requirements

Risk monitoring can be considered as the most important component of risk management for risk identification. This of course does not mean that the rest of the risk management component is negligible, but the fact is that without risk identification and risk monitoring other risk management components cannot be realized or may be realized poorly. Risk monitoring is important for the correct choice of methods, which provide all or most tools for measuring risk of occurrence for the specific facts and measuring timely risk probability and detecting impact of change. Traditionally, control theory is described in some mainstream risk monitoring methods, but these methods cannot cover all the risks of the project[5].

Risk monitoring methods, as well as the response to the risk are an integral part of risk management planning. At the same time risk monitoring methods may lead to the development of metrics to drive when certain parameter values. For example, the values can be values obtained from analysis of deviations from the index 1 (potential allowable value). Risk monitoring is important to assess what are the sources of information for monitoring risk[6].

Process management literature[5] is also mentioned in the reserve analysis (Reserve Analysis). Reserve analysis is performed according to what risk can occur. Occurrence of risk is influenced by the timing or cost. Reserve analysis is estimated and compared if actual reserve balance coincides with the projected reserve balance. Reserve analysis can be combined with the values obtained from the analysis of the assessment indexes. Similar to the values obtained from the analysis – also in the reserve analysis is recommended to use any of the computer applications.

An effective method to avoid risks or minimize the risk impact is a regular risk analysis of the causes and characteristics. Risk analysis of the causes is of an important source of information about the external and internal environment, various expert reports and forecasts[7].

Similar to risk identification, risk monitoring can be used for expert methods. Experts estimate execution time to re-evaluate project risks, analyze the causes and risk characteristics. Experts can assess already identified causes and symptoms, new causes and identify new symptoms, as well as use information about the progress of the project to identify new risks. Experts use similar methods as an expert who identifying risks. The only difference from other methods would be hamstrung by the simplification of expert methods.

Risk response is not the only risk management component, it occurs during execution, but it is also a process, which takes place during the planning phase. Risk is a complex reaction, when numbers of interrelated steps are carried out. Preventive actions are intended to avoid or reduce the risk or the impacts of risk, i.e., activities are carried out in a timely manner or proactively. For example, when the values obtained from the analysis indicated that the coefficient of variation of 1 has not yet reached a critical value, but the deviation is detected (α) (see. Fig.1).

Activities are often carried out without waiting for the critical values to be achieved. Plan to determine the causes of risk in case of detection, preventive action can be recommended for risk analysis of the causes and characteristics. But complex activities are usually carried out after the occurrence of the risk, as there is a need to respond to the risk consequences. It should be emphasized that the development of risk management can be done in two ways.

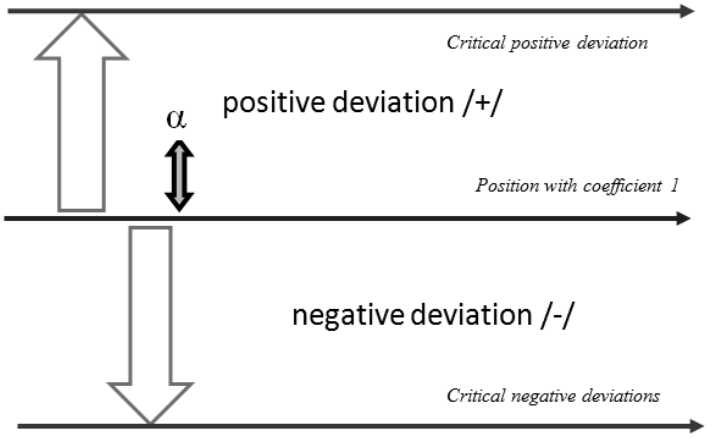

Fig. 1. Risk analysis of the obtained value of significance.

First, the organization develops risk management gradually improving each subsequent degree of realization as compared to the previous one. It may be just the risk management process improvement or organizational, team, system management maturity growth component. Second, risk management can be improved in certain system actions during implementation.

4. A possible solution to the problem

Activities are often carried out without waiting for the critical values to be achieved. Plan to determine the causes of risk in case of detection, preventive action can be recommended for risk analysis of the causes and characteristics. But complex activities are usually carried out after the occurrence of the risk, as there is a need to respond to the risk consequences. It should be emphasized that the development of risk management can be done in two ways. First, the organization develops risk management gradually improving each subsequent degree of realization as compared to the previous one. It may be just the risk management process improvement or organizational, team, system management maturity growth component. Second, risk management can be improved in certain system actions during implementation.

So it can be said that overall risk management is coordinating activity, the task is to direct and control the activities of the organization and process, taking account the notable risks. The whole complex process can be expressed in the sequence of events that justify and demonstrate the need for risk analysis (see. Fig. 2).

Although risk management is described as relatively simple process, the problem of a suitable choice of terminology has to be considered and fully characterize a given system, the potential risks by nature. Realizing the threat model, this model should be described as a complex object infrastructure, which has already designed and embedded security features based on pre-existing practices and research.

Social networking can be described in at least three layers / levels – technological ontology, ontology entities (in the sense of the subject, users socially - psychological characteristics) and communicative ontology as different semantic levels. In today's social networking activity, despite the fact that it is designed and operated to set the security elements that are associated with the emergence of new threats and vulnerabilities, common findings indicate specific range of characteristics.

The common threat model (which can be attributed to social networks) and preventive measures are offending external and internal factors. Themes in relation to the concept of "offender" are understood by person who uses social networks for harmful and / or illegal activities, with the aim to benefit (economic, social, psychological). The social network is selected as the means of achieving this for the reason that it brings together most of the country's population (there are exceptions) or friendly, committed acquaintances that create a false sense of security for users,

while the possibility to spread information on social networks gives a high target coefficient – it can often be impossible or very low likelihood to achieve it in the physical environment.

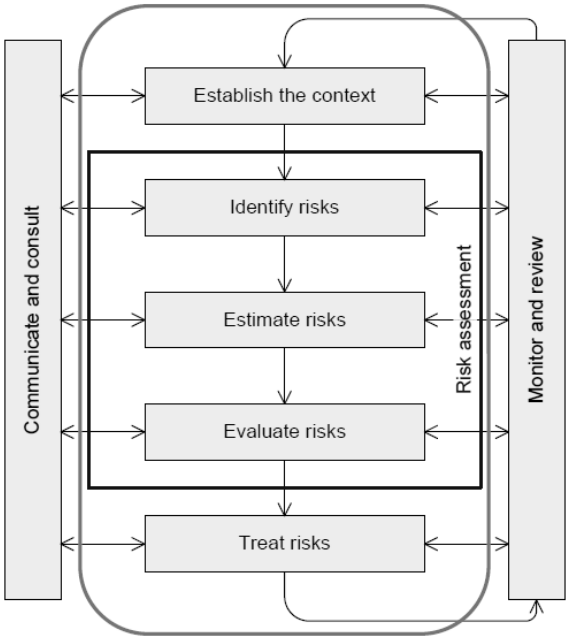

Fig. 2. Risk analysis components [adapted from[8]].

At the time when the offender has chosen social networking as a target environment, the likelihood of threat exceeds level of 0, which means that the threat of the occurrence of the indicator changes from "impossible" to "possible." Violators' have chosen social network because it is a favourable environment to reach persons and disseminate false and distorted information in a rapid way (fake profiles, fictional activities, promotions, fake companies, fictional charity projects). Social networks have formed a picture that includes the belief that it is impossible to maintain complete anonymity on the Internet, easily distribute false or partly true information.

Initially, the threat spreads using process of building information „package" that spreads over the information space of social network. Social network's transmission of information is tree-like. For qualitative changes of social networking in the future, it is essential to find an indicator that allows one to manage the threat of information flow on social network with high probability, since the dissemination of fictional information on the social network is a threat to further joining such networks (by obtained private data users are involved in illegal activities, misused funds obtained from fictional charities).

When solving the problem of the prevention of threats within social networks, complexity of predictability and management of threat should be emphasized; as one user distributes information to some other group of users, others circulate it.

One solution is to build a "barrier" at a time when the threatful information "package" moves from one group / type of profiles to another (children transferring information to adult, adult transferring to a teenager).

In the research is important to ascertain CORAS for completely describing social networking facilities, links and interactions. Social network structure can be described using an ontology-based approach, which is an important aspect of the threat classification, threat identification from network user's profile socio-psychological portrait (pre-school, primary school, teenagers, young adults online, seniors, considering age, gender and other criteria defined in the study).

Threat occurrence and spread is defined in the light of class objects, links and exchange of information provisions of social networking ontologies, there is no doubt that social networks, like any human community, is a system that can be described as socio-technical.

5. Conclusion

Along with more users joining social networks, possibility of threats is growing, as the information can be reached by expanding number of individuals that increases the possibility that the information „package" will find their way to their subjects with the appropriate degree of sensitivity to the information – vulnerability.

Therefore, the risk management process and, in particular, the risk identification and analysis of key characteristics should be performed, using which it is possible to describe threats, causes and types of social networks as an information system:

- Threat – a threat the nature of which can be described as a single element or as a set of elements;
- Vulnerability – system component that can be influenced in a desired or undesired manner;
- Unwanted incident – threat resulting in an event that causes injury, damage, it is not desirable in the system;
- Risk – the possibility that the threat will happen using the system and adverse event occurs;
- Treatment – in the sense of risk prevention, mitigation measures to prevent adverse event.

Risk management theory provides the risk management methods to the study and the author concludes that it is essential for the practical application of risk management to information systems to use visual methods. In turn, realizing the scientific work, the found method is to be internationally known and understood, the terminology should be created. One of these methods could be CORAS because CORAS is a method for conducting security risk analysis. This method provides a customized language for threat and risk modelling. CORAS is model-based and the Unified Modelling Language (UML) is typically used to model the target of the analysis. Therefore CORAS could be used for threat and risk modelling in social networks to find out possible solutions to minimize the risk.

References

1. ISO 31000: Risk management. Retrieved: 01.08.2014, URL: http://www.iso.org/iso/home/standards/iso31000.htm
2. Karimi, A.A., Mousavi, N., Mousavi, F., Hosseini, S. Risk assessment model selection in construction industry. *Expert Systems with Applications* (38), 2011. p. 9105-9111.
3. Krane, H.P., A. Rolstadas and N.O.E. Olsson. Categorizing risks in seven large projects-Which risks do the projects focus on? *Project Manage*. J., 2010. 41: 81-86.
4. Berg, H.P. Risk management: Procedures, methods and experiences. *Risk Manage*, 2010. 1:79-95.
5. Pinto, J., Cleland, D., Slevin, D. The Frontiers of Project Management Research. Project Management Institute, 2003. p.503.
6. Smith, P. Merrit, G. Proactive Risk Management. Productivity press, 2002. p. 248.
7. Brandon, D. Project Management for Modern Information Systems. IGI Publishing, 2006. p. 417.
8. Stølen, K. The CORAS Method. Process, Concepts and Notation. SINTEF, 2011. p. 27.