Research on Security Risk Management Process

Peiqi WANG,Yu WEN
Defence Science University , P.R.China
463872349@qq.com

Abstract Starting from the concept of risk, security risk and security risk management, this paper analyzes the research status of security risk management. Five key links of security risk management are introduced: security risk planning, security risk identification, security risk assessment, security risk response and security risk monitoring. In order to provide theoretical countermeasures to deal with security incidents.

Key words Security risk management, Process

1 Introduction

It is the best time to explore security risk management. There are many kinds of crisis all the time. It is effective to predict the risk and take corresponding countermeasures before the crisis. As the field of security management and risk management theory, it is necessary to study the process of security risk management, how the face significant events in a step-by-step implementation of the security risk management.

2 Basic Concepts

2.1The risk

Because of the different understanding of risk, there is no uniform definition of risk in academic circles.Economists, statisticians, decision theorists and insurance scholars have four main concepts of risk: risk is the uncertainty of loss[1]Risk refers to the possibility of loss, the deviation between actual result and expected result, and the probability and consequence of actual result deviating from expected result[2]. The modern Chinese dictionary (edition 6) defines risk as a possible risk[3]. Weber's definition refers to the possibility of injury, injury or loss. The interpretation of risk by the relevant agencies of the us congress is the possibility of specific consequences, usually adverse consequences in a specific situation. The UK risk report explains that uncertainty about the outcome of actions and activities can be a positive opportunity or a negative threat. The new definition of risk is that risk is the effect of uncertainty on goals.The definition emphasizes the following three points: risk is an influence, which may be positive or negative, that is, risk may be an opportunity to generate benefits; It could also be a threat, causing damage. Risk is for specific goals. In risk management, there is no risk without goals.It can be seen that risk is essentially the uncertainty of loss, manifested in the possible loss or such loss is uncertain.The uncertainty is also manifested in the occurrence of uncertainty, occurrence of time uncertainty, occurrence of space uncertainty, occurrence of process and result uncertainty.

2.2 Security risk management

The literature shows that experts and scholars in the field of management have a consistent definition of security risk management, mainly exploring the connotation of security risk management from the

perspectives of security management and risk management. Security management of colleges and universities teaching material about the definition of security management is representative, it is defined as: for the realization of the system security, using the principles, methods and principles of management, analysis and research all kinds of unsafe factors, involving human, material and financial resources, such as information security resources to make decisions, plan, organize, command, coordination and control of a series of activities, in order to reduce and eliminate all kinds of unsafe factors, prevent accidents[4].Production security risk management and control of risk management of interpretation is as follows: risk management is risk management main body through the risk identification, risk assessment, risk control, to control the risk effectively and properly handle the loss of process[5]."Based on the information system of the command effectiveness evaluation and risk management of risk management, this paper is: the risk management in addition to the planning, organization, coordination, command and control function, also has its own unique features.At its core, it reduces losses.From the perspective of the management body, it can be an individual, or it can be a unit, enterprise and military organization at all levels.From the perspective of its process, it is a dynamic process of continuous decision-making by managers[6].

Risk management in system security as the goal, is the quantitative identification of risk factors and hazards, accident prevention and control, in the security management have played an important role relations globally, the key to the future, is the core of security management. The purpose of risk management is to detect and identify the risk factors that may lead to the accident in advance, so as to take measures to eliminate and control these factors before the accident and prevent the accident. In a sense, risk management is an innovation, which develops from the traditional security analysis and security management.Security risk management is to use the methods and means of risk management, a systematic analysis of various kinds of risk factors, the size of the possibility of assessing risk, targeted to eliminate hidden dangers and to resist the threat of countermeasures and measures, prevent and avoid the security risks, risk control at the lowest level, so as to maximize ensuring the security of personnel, equipment, materials, etc.

ISO 31000:31000 "issued by the international organization for standardization of risk management - principles and guidelines define the risk management as" against risk taken by the command and control organization to coordinate the activities of ", that "the risk management process" is the management policy, procedures and methods systematically applied to the communication and consultation, to set up the environment, as well as the identification, analysis, evaluation, response, monitoring and review of the activities in the process of risk.

3 Key links of security risk management

On the basis of domestic and foreign research on the operation process of security risk management, adjustment and improvement are carried out. The optimized operation of security risk management consists of five steps: security risk planning, security risk identification, security risk assessment, security risk response and security risk monitoring.

3.1 Security risk planning

Security risk planning is the starting point of the security risk management work, is also a security risk

management organization can have goals, plans to complete its tasks of a whole package, make the security risk management work to cooperate more closely, run more smoothly.

Security risk planning should include six main elements in programming.One is the introduction. Explain the overall goal of security risk management and the objectives of phased tasks, and define the schedule and major time nodes of security risk management. Second, the organizational part of security risk management. First for security risk management organization structure, personnel deployment are described in detail, make sure you are able to accurately find out the security risk management by which organization, which is a part of personnel to be responsible for; Secondly, personnel should be divided into tasks in a systematic way according to the attributes and professionalism of organizations at all levels. Finally, the functions of the organization should be clarified to ensure that the organization can fulfill its responsibilities and improve efficiency. Third, the identification part of security risk management. According to the basis of security risk identification, use the appropriate security risk identification method to find out the existing security risk hidden danger. Fourth, security risk management assessment. Firstly, the index system of incident security risk assessment should be constructed according to the actual situation.Secondly, through the method of security risk assessment, the weight value of each security risk hidden danger is quantitatively analyzed. Finally, by combining qualitative and quantitative methods, the harm degree of each security risk hidden danger in the event is arranged.Fifth, the security risk management response part. According to the result of security risk assessment and security risk prevention coefficient values, use what kind of strategies can effectively control risk, prior to list all the hidden trouble of security risk coping strategies. The sixth part is the monitoring part of security risk management. It mainly monitors the smooth operation of security risk management organizations and the effective implementation of security risk management. The seventh part is the appendix. Further explanation and explanation are given to the additional contents in the security risk planning scheme.

3.2Security risk identification

The main content of the security risk identification is relying on the security risk management leading group and outside experts, using proper security risk identification method, a comprehensive system of security risks that may exist in the process of hazard identification and summed up, to lay the foundation for subsequent security risk management work.

At present, there are many mature methods for security risk identification, and the main representative methods are Delphi method, brainstorming method, fuzzy fault tree analysis method, twilight analysis method and SWOT method.The five kinds of security risk identification method in use, advantages and limitations of compare analysis, in the process of carry out according to the actual situation to choose the right method to identify the security risks of job.

3.3Security risk assessment

In security risk identification phase, preliminary establishes a major security risk factors influencing events, so the security risk assessment phase of the main work, is according to the different types of security risk factors in selecting the appropriate evaluation method, with the method of combining quantitative and qualitative, to assess the security risk factors of damage degree and influence scope, the security risk management according to the results of the assessment, selection of an optimal response, effective control of the security risks existing in the implementation.

Security risk assessment is based on the identified all kinds of security risk factors are qualitative analysis,

refined into specific indicators, combining the theory of probability and mathematical statistics, mathematical model of the quantitative indicators, and predict the influence of security risk factors, to evaluate the overall level of security risks. The content of security risk assessment mainly includes four aspects: one is to analyze the level of security risk. In the work of security risk assessment, the most basic content is to be able to analyze the probability of various security risk factors evolving into accidents. Only when security risk factors are sorted and compared according to the probability of occurrence of accidents can they be classified and controlled and avoided.The second is to analyze the possibility of security risk accidents. Before starting, the characteristics and laws of security risk factors are analyzed through security risk assessment, and the possibility of environmental transformation into security risk accidents is predicted. Third, analyze the correlation of security risk factors. Behind any security risk accident, not only there is a security risk, through the security risk assessment work analyzes the correlation between the security risk factors, so as to protect against it without missing. The fourth is to analyze the degree of harm after the occurrence of security risk accidents. By setting the assumed conditions, the paper analyzes whether the security risk factors are within the acceptable range of the participating troops after the accident changes and whether they will cause serious damage to the overall security.

3.4 Security risk response

Security risk management of the overall goal is to security risks effectively controlled in the range of acceptable; therefore on the basis of the security risk identification and evaluation, work out the response contains all possible conditions, in order to achieve rapid hidden trouble of security risk in the process control. At present there are five kinds of commonly used security risk coping strategies, risk retention, evade, prevention and mitigation and transfer, combined with the actual situation, choose appropriate strategies according to different risk.

Risk retention means that the undertaker can accept the loss caused by the security risk and choose a risk disposal method to be undertaken by himself.As the frequency of the security risk is higher but the loss of small, or choose other risk control strategies consumption costs are much higher than the security risk losses, can consider to choose the way risk retention.

Risk aversion refers to trying to avoid possible security risks under the action of decision-making instructions. There are two common ways. One is to analyze the possibility of the security risk problem in advance, and make reasonable disposal of the hidden security risks before the problem occurs. The other is that the known security risk problem will cause irreparable loss and cannot be avoided. Therefore, it will choose to change the action plan or abandon the original plan to avoid the risk.

Risk prevention refers to the indirect prevention of security risk problems by means of engineering blockage, behavior guidance and institutional constraints. Engineering blockage is to use the way of human intervention to block the connection between the risk source and the risk source. Behavior guidance is to use education, publicity, training and other methods to prevent security risks caused by unsafe behaviors of personnel.System constraint is to avoid the occurrence of security risk problems by using the constraint of rules and regulations.

Risk mitigation refers to the concentrated reduction of the incidence or harm of certain security risks and risks, so as to achieve the overall security risk mitigation effect. The purpose of risk mitigation is a major power concentration, for the security risks identified mitigation strategies, using the characteristics of the security risk to pass each other and influence each other, reduce security risk overall loss rate.

Risk transfer refers to the transfer of the source of risk to a third party, or the loss caused by the risk to other places.The common form of risk transfer is to take the local departments concerned as the responsible party of all or part of the risks, and effectively reduce the pressure to bear the security risk loss through the intervention of local departments.

3.5 Security risk monitoring

The security risk is changing dynamically, and even if corresponding measures are taken to deal with the possible security risk problems, it cannot indicate that the security risk has been completely eliminated.Should actively play to the role of the security risk monitoring, as well as adopted by the security risk problem of security risk response to check and feedback, also want to work for security risk management of the overall implementation in real time supervision.

Security risk monitoring is generally the responsibility of the supervisory group in the security risk management organization structure.Its main work content has two, one is to carry on the track investigation to the security risk question. When the security risk management for a security risk to the security risk response, teams will follow up in time, the problem is a full range of inspection, to ensure the security hidden trouble has been effectively control risk.If the security risk problem is properly controlled, the specific process of its disposal should be written into the security risk monitoring report as the data reserve of security risk management.If there is a new change in the security risk condition, it is necessary to carry out the whole process of security risk management again for the new security risk hidden danger.

The other is to monitor and supervise the efficiency of the implementation of security risk management organizations. Whether the security risk of planning stage, identification stage, evaluation stage or in the face of the stage, all has the direct influence on security risk management activities, and the security risk monitoring is to security at various stages of risk management for the supervision of the inspection. Through the way of performance evaluation of responsible for each stage of the task to examine the organization and personnel, identification of risk factors for whether a comprehensive, the evaluation of the level of risk, risk of countermeasures to choose whether or not appropriate, etc. The key node to focus on supervision and evaluation.In security work summary, for the security risk management tasks to complete the high efficiency of organization and individual should be given certain reward, to stimulate enthusiasm and reduce the probability of security risk problems.

4Conclusion

When dealing with major events, such as natural disasters, anti-terrorism, military exercises and other activities, new management of the process of security risk management can be applied to ensure that the accident rate is minimized.It should be pointed out that, in the paper from the perspective of theory, this paper emphatically analyzes the security risk management countermeasures, in the actual operation, there are many quantitative methods can be used, this also is the main content of further research.

References

[1] Xu jinliang. Risk management [M]. Beijing: China finance press,2006.1-3.

[2] Yu qiaohua. Efficient security management of the armed forces -- an analysis of 50 typical cases [M]. Beijing: long march press,2013.231-232.

[3] Dictionary editing room, language institute, Chinese academy of social sciences. Modern Chinese dictionary (edition 6)[M]. Beijing: commercial press,2012, 390.

[4] Wang kaiquan. Security management [M]. Beijing: chemical industry press,2011.8-9.

[5] Chen shaorong. Security production risk management and control [M]. Beijing: chemical industry press,2013.8-9.

[6] Cheng qiyue. Command effectiveness evaluation and risk management based on information system [M]. Beijing: national defense university press,2011.286-287