Analysis of changes in the probability of an incident with information security

Petko Genchev
Computer Science and Engineering Department, Technical University of Varna
Varna, Bulgaria
P.Genchev@tu-varna.bg

Abstract: *Risk assessments are not a one-off action, but there are no formal guidelines on when and how often a risk assessment should be performed. Changing factors affect the risk assessment parameters. The strongest influence of these changes is the probability of an accident. Examining changes in the likelihood of an accident will allow for more accurate planning of periods for checking risk factors and assessing risk. In this way, the assessed risk will reflect the changes that have taken place and will lead to more adequate risk management. The analysis of the influence of the changing risk factors is made with the help of a model, which is built on the basis of one asset and the accident scenarios determined for it. The model examines the characteristics of changes in the risk factors for the asset. The probability distribution for the random number of changes is determined. The results of the amended conditions are also random. They are expressed in a change in the level of probability of an accident. For these random variables, the main probabilistic characteristics are determined and dependencies are derived that can be used for analysis.*
Keywords*: INFORMATION SECURITY, RISK ASSESSMENT, DYNAMIC SYSTEMS AND CONTROL*

1. Introduction

According to ISO/IEC 27005 standart[1], in the process of information security risk assessment for each asset, all threats and vulnerabilities to the asset are identified. Vulnerability is mapped to each threat and thus incident scenarios are identified. In this sense, an incident means a threat that has attacked a vulnerability and led to a negative impact on the asset. After determining the incident scenarios, using qualitative and quantitative methods, the levels of probability of realization of the identified scenarios are determined, as well as the levels of impact that each incident may have on the asset. The level of risk is determined by the probability of each scenario and the impact of the incidents. It is a snapshot of the risk to the asset because the assessment was made under certain conditions for the asset. Over time, the conditions for the asset change and it is therefore possible that the probability of an accident and the impact of the incident may also change. Changes in conditions affecting the level of impact are largely deterministic and can be reflected in the level of risk. But the change in the conditions for the realization of accident scenarios is a random variable. This should lead to a change in the level of risk. Of course, in the event of a change in the impact, there are accidental impacts, but the process of change is slower and more determined than that of changing the conditions for an accident.

It is therefore very important to periodically check the risk factors and, if necessary, to re-determine the level of risk. There are no officially defined guidelines on when and how often a risk assessment should be performed. There are recommendations for more frequent reviews of the level of risk in case of significant changes in the subject of activity of the organization, improvements that have been made in the organization, problems arising from the task, incidents or omissions. It can be summarized that the security risk assessment should be a continuous activity. For critical information systems, it is highly recommended that a more frequent security risk assessment be performed.

The ISO/IEC 27004 standard [2] provides recommendations for periods of verification of the effectiveness of applied controls. This can serve as a basis for determining the periods for checking the risk factors for a group of assets. In most cases, verification periods are recommended by experts based on statistics from insurance companies and government statistical organizations.

The frequency of inspections depends on the type of asset and other factors and a simplified approach is needed to easily determine the frequency of inspections.

The purpose of the material is to make an analytical model of the process of changing risk factors to determine their influence on the value of the probability of an accident.

The article is structured in 4 parts: introduction, analysis of the influences of the changed risk factors on the probability of realization of an incident, the analysis of the changes of the probability of an incident and conclusion.

2. Analysis of the influences of the changed risk factors on the probability of an accident

2.1 What are the risk factors?

The ISO / IEC 27005 standard [1] defines some of the risk factors such as asset value, impacts, threats, vulnerabilities, probability of occurrence. It is determined that they should be monitored and reviewed in order to identify any changes in the context of the organization at an early stage and to have an up-to-date view of the overall risk picture.

It is necessary to monitor the new assets included in the scope of risk management, the necessary modifications of asset values, the emergence of new threats inside and outside the organization, the emergence of new or increased vulnerabilities, the emergence of new opportunities to exploit vulnerabilities, increased impact, as well as information security incidents.

2.2 Objectives and statement of the task

In the process of changing the level of risk, the greatest influence is exerted by the probability of an accident. In addition, this element of the level of risk changes most dynamically. From this point of view, it is important to study the rate of change and the levels of change in the level of probability of an accident.

The possibility of realizing accident scenarios represents probability I0 at a certain moment and the change of conditions over time. It is important to determine the period for checking the conditions. Changing conditions will lead to a change in the probability of an accident at the end of the period. An acceptable level of probability level is defined in the risk assessment methodology approved by the

organization. This value can be used for a limit value Ilimit, up to which the level of probability may increase with changes in conditions. The difference Ilimit - I0 will determine the amount of allowable change in the probability depending on the changes in conditions during the time between two inspections.

It is important to determine the parameters influencing the determination of the period for inspections of risk factors. The size of the period must ensure that the probability of an accident changes within the allowable probability value.

We will consider the following statement. For a period of approximately one year, it is assumed that there are n incident scenarios defined for an asset. It is also assumed that the dynamics of the emergence of new scenarios is less than the dynamics of changes in the described scenarios and will not affect the objectives of the analysis.

2.3 Mathematical model

Within one year, changes in probability characteristics may occur in none, one or more of the scenarios. Depending on the case, this number may be different and should therefore be considered as a random variable K with some probability distribution:

(1) $P_k = P\{K = k\}$, за к=0, 1, 2, ...n

There are various hypotheses about the probability distribution of such a random variable. One of them can be synthesized as follows. Let q denote the probability of a change in the conditions for the individual scenarios and assume that it is the same for all scenarios. Independence of changes in the conditions for all scenarios is assumed. In this situation, the number K of changes during the year represents a random variable with binomial distribution:

(2) $P\{K = k\} = \binom{n}{k} q^k (1-q)^{n-k}$

With such a distribution, the average number of changes in conditions per year will be equal to nq, with a variance of nq (1-q) [3].

It is known that the binomial distribution with a small probability q is quite close to the Poisson distribution with parameter $\lambda = nq$ [3]. So another possibility for the distribution of the number K of changes during the year is that of Poisson:

(3) $P\{K = k\} = \frac{\lambda^k}{k!} e^{-\lambda}$, за к = 0,1,2, ... ,

with mathematical expectation λ and variance also λ [3].

The use of the Poisson distribution allows overcoming some technical difficulties and therefore in further consideration we will use it as an example for the distribution of the random variable K.

As a result of the changes in the conditions for realization of the scenarios, an addition to the probability of an accident in a given scenario is formed. The size of the additive, and hence the risk to the asset, varies from case to case and it is logical to consider it as a continuous random variable X. It is often hypothesized that this random variable has an exponential distribution with intensity ξ [4].

(4) $P\{X \geq x\} = e^{-\xi x}$

In this situation, the average size of the additions to the probability of an accident in the individual scenarios is 1/ξ , and the variance is 1/ξ^2 .

An important hypothesis for the further construction is that for the different incident scenarios the changes are independent random variables and do not depend on which other scenarios an additive has occurred, nor on the number of scenarios.

The sum of the additives during the year is random variable and the asset may be at risk if these values exceed a certain critical level.

Therefore, studying the distribution of the annual additives to the probability of an accident could contribute to clarifying the risk management policy for the asset.

What is special about considering the annual amount of additives is not only that additives are random, but also that their number is also random:

(5) $Z = X_1 + X_2 + \cdots + X_k$, for K>0 and $Z = 0$, for K=0

The mathematical expectation of the sum is relatively easy to find. The notional average value, provided that K has a certain value, is the sum of the average values of the individual collectibles:

(6) $E(Z) = \frac{E(K)}{\xi} = \frac{\lambda}{\xi}$

The variance is obtained analogously as a sum of independent random variables .:

(7) $D(Z) = \frac{D(K)}{\xi^2} = \frac{\lambda}{\xi^2}$

3. Analysis of changes in the probability of an accident

The development of the probability of an accident for an asset is determined directly by two factors. First, from the initial level of probability, the size of which determines one or another starting position of the risk for the asset. And second, from accidental additions to the probability of an accident over a period of time.

The initial level of probability of accidents is defined in the risk assessment of the asset and represents the initial value of the probability, which can be changed until the next check. The change in the probability of an accident until the next inspection is due to accidental changes in the risk factors for this asset in the period between inspections. This element of the total probability of an accident has the possibility to add or subtract from the value of the probability of an accident. We will be interested only in the added value, because only it leads to an increase in the risk for the asset.

Let us consider a situation in which checks of risk factors are made during period ***t***. If there are no changes in the risk factors for the asset, there will be no formed addition to the probability of incidents with the asset. Then at the end of the period between inspections we will have a probability I_t with the same value as at the beginning of the period I_0 .

The appearance of changes in risk factors will lead to the formation of an addition to the probability of an accident at the end of the period. As it has already become clear, this quantity is the sum of a random number ***K(t)*** of random variables $X_1, X_2, \ldots X_{K(t)}$:

Then, at the end of the period between inspections, we will have the possibility of an accident

$$(8)\quad I_t = I_0 + \sum_k^{K(t)} X_k$$

The random variables $X_1, X_2, \ldots X_{K(t)}$ are assumed to be independent and with the same distribution with mathematical expectation μ and variance σ^2.

Suppose that the number of additives for a period from ***0*** to ***t*** as an average value accumulates at a constant rate $E(K(t)) = \lambda t$. . In this case, the mathematical expectation of the annual size of the additions to the probability of an accident would be $\lambda\mu$,, and for the total value of the probability of an accident as a mathematical expectation will apply:

$$(9)\quad E(I_t) = I_0 + \lambda\mu t$$

Where: $E(I_t)$ is the total level of probability of an incident with the asset, which is accumulated for time ***t;*** I_0 is the initial level of probability of an asset incident; λt is the number of changes for time ***t*** , which represents average rate of accumulation; μ is a mathematical expectation of the size of the additions to the probability of an accident. This shows how much the probability of an accident changes on average

Then the average increase of the additives to the probability of an accident for time ***t*** is $\lambda\mu t$. If the value of $\lambda\mu$ is positive, the value of the additive will increase, albeit only as an average value, as a general trend, where fluctuations up and down are possible. Otherwise, if $\lambda\mu$ is negative - the addition to the probability of an accident will decrease, although again only as a trend in the average value.

At $\lambda\mu t. < 0$ we have a situation in which over time the probability of an incident with a scenario decreases. This is a positive trend to reduce the risk to the asset. This trend should have little impact on the risk monitoring process, as it does not reduce the inspection period. However, reducing the likelihood of risk should not automatically lead to an increase in the time between inspections. It is necessary to conduct an expert analysis of the causes of this phenomenon and to take steps to increase the time between inspections only after establishing a lasting trend to reduce the likelihood of an accident. The value of the variable $\lambda\mu t$ is a function of the changes in the conditions of several events that have different trends and they must be tracked. Even if an event reaches probability ***0***, the threats and vulnerabilities that determine it must be monitored for new trends to emerge. In addition, the current analysis of the required verification period is made on the assumption that the dynamics of new scenarios is low, but this does not exclude the possibility of new events (threat-vulnerability). Therefore, the decision to extend the period for checking the risk factors for the asset in question must also take these factors into account.

If $\lambda\mu t. > 0$ we have a case of increasing probability of accidents. This is the situation that should have a major impact in determining the inspection period. The following cases need to be considered:

• For $I_0 \geq I_{limit}$ we have a calculated probability of an accident that is equal to or greater than the acceptable level of probability for this asset. This assumption is unlikely because in such a situation risk mitigation measures are taken to reduce the risk below the acceptable level. It is possible to reach this situation at a very high cost of reducing the level of risk and deciding to accept the high level of risk. In this case, the periods for checking the risk factors should be determined by the management of the organization with the assistance of risk management experts.

• When $(I_0 + \lambda\mu t) \geq I_{limit}$ there is a very high rate of increase in the probability of an accident, which for time ***t*** leads to an increase in the probability of an accident above the specified acceptable value of the probability level. In this case, the period for checking the risk factors must be reduced to values where the acceptable level of probability is not reached. Simultaneously with the reduction of the inspection period, it is necessary to conduct an analysis to take measures to reduce the rate of increase in the probability of an accident. In Fig. 1 this situation is illustrated with values above the ***Ilimit*** value.

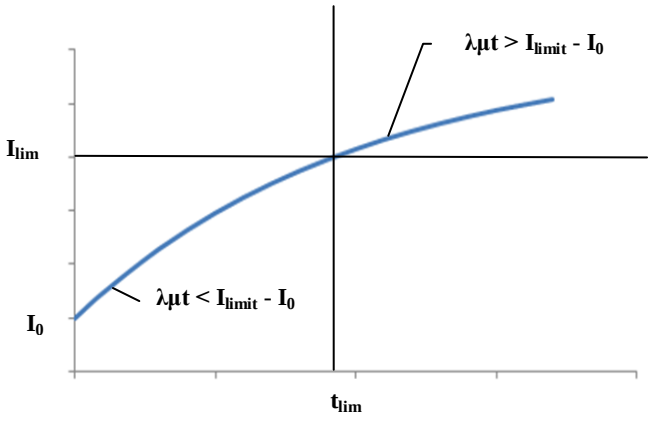

Fig. 1 *Change in the probability of an accident*

• At $(I_0 + \lambda\mu t) < I_{limit}$ we have a situation of a normal rate of increase in the level of probability of an accident due to changes in risk factors. In this case, it can be assumed that an acceptable period of inspections has been set. . В илюстрацията на фиг.1, това е периода в границите от ***0*** до t_{limit}.

In the defined period, the risk factors are checked and the level of risk is determined. The performed inspection serves as a starting point for determining a new period for performing the next examination of the risk factors.

4. Conclusion

The material is a model of the influences and dynamics of changes in risk factors in determining the risk to information security of an asset. The probabilistic characteristics of the changes are determined and the main dependences that can be used for analysis are derived. Based on the identified dependencies, the change in the probability of an accident is modeled and analyzed. Conclusions are made about the relations between the probabilistic quantities and the intensity of the changes.

The analysis used the statement and characteristics of the risk assessment process for information security, but the conclusions can be used for the needs of risk assessment in other risk management systems.

The models made and the derived dependencies can be used to analyze and define an approach for determination of the periods for checking the risk factors.

5. References

[1] INTERNATIONAL STANDARD ISO/IEC 27005:2018, “Information Technology-Security Techniques-Information Security Risk management”, Reference number ISO/IEC 27005:2018(E).

[2] INTERNATIONAL STANDARD ISO/IEC 27004:2016, „Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation”, Reference number ISO/IEC 27004:2016..

[3] Людмил Цанков, “Вероятности и физическа статистика - записки на лекции”, “Probabilities and physical statistics - lecture notes”, Sofia, 2011г., look at http://ntne.phys.uni-sofia.bg/BG/Manuals/PS.pdf

[4] “Събития, инциденти, случайности, опасност и риск”, "Events, incidents, accidents, hazards and risks", look at http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj81vTSk5TuAhUHfMAKHVJmB7E4ChAWMAN6BAgEEAI&url=http%3A%2F%2Fspaska.lirex.net%2Fins-educ%2Fbook-1%2F04.pdf&usg=AOvVaw2_uboSA0ac8YsvR7RYdABh