SocioBrains
ISSN 2367-5721, JOURNAL HOMEPAGE: WWW.SOCIOBRAINS.COM
INTERNATIONAL SCIENTIFIC REFEREED ONLINE JOURNAL WITH IMPACT FACTOR
ISSUE 42, FEBRUARY 2018

RISK ASSESSMENT IN CYBER SECURITY SYSTEMS

Abstract: This article is an attempt to systematise published common frameworks for cyber security system risk assessment with the aim of supplementing and developing the existing methodologies.

Author information:

Kamen Kalchev
Associate professor Ph.D.
Department: Communication and Information Systems
Military Academy "G.S.Rakovski" – Sofia
✉ kamenstanev@abv.bg
Bulgaria

Keywords:
cyber security, risk, risk assessment, Cybersecurity Framework, ISO- 27001, NIST SP 800-53.

The unprecedented development, and proliferation, of information technologies is impressive not just with its scope but also with its capacity to permeate an ever larger part of our lives. It is often pointed out as a reason for the profound, largely positive changes in economy, social life, education, science and culture. Information technologies have formed their own cyberspace, described as a parallel dimension to the physical world, and have made it possible for all our activities to become freer, more mobile, faster and somewhat less responsible [1].

Internet users are more than 2.3 billion. As a result, the impact of the worldwide web on social life and economics is growing incredibly, which leads to the appearance of threats new both in form and essence. Due to the ubiquitous use of information technology, securing the information in a system is acquiring a great importance. The Internet has become not just the largest information bank, but also a place where a considerable potential is being focused of crucial government and corporate management infrastructure. Along with this, the Internet also has an increasing impact on national security.

Despite the positive impact of information technology, over the past years we have witnessed the huge destructive effect, both direct and indirect, it can have. Some of the most prominent examples in this respect are the information leak from the WikiLeaks website, the Stuxnet virus attack on Iranian nuclear facilities, as well as the possibility of provoking unrest and full-blown conflicts through social networks.

The numerous cyber attacks which take place daily on the worldwide web, as well as the growing interest in issues of security, force a large number of organisations to change their approach to security. For a start, they take into account the fact that complete protection is impossible in view of the open nature of the information processes implied in the interaction with partners, shareholders and clients. Secondly, more and more organisations are following common or standardised guidelines to offset unforeseen losses though determining the risk they are facing.

In addition, according to a 2017 PwC (PricewaterhouseCoopers) security survey [2] which interviewed more than 9000 business executives from around the world, more than a quarter of those involved do not know how many cyber attacks their organisations have been subjected to, and a third of those who are aware of the cyber attacks which have occurred do not know how they have occurred. Another interesting fact is that more than a half of all cyber attacks are caused by general security failings which can easily be prevented with good management.

In view of this, one of the important steps an organisation can take in order to improve its IT security is to undertake a thorough assessment of the risk of cyber attacks. This would undoubtedly allow it to overcome the high level of indeterminacy in foreseeing such attacks and also to reduce considerably the potential losses caused by mismanagement.

Where the term is used, various definitions of risk exist, some of which do not require establishing a precise correlation between likelihood and implications. Others unambiguously determine risk through the existence of such a correlation. However, all definitions presuppose proportionality between likelihood and implications.

The definition made by Blaise Pascal says 'risk should be proportional to the probability of occurrence as well as to the extent of damage'. [3]

In IT security, the following definition of the term risk (K) is used: it is 'a function of the likelihood of occurrence of an unwanted event (P) and the losses (C) which would be incurred if it arises' [4].

$$K=P*C$$

In the theory of decision making, risk (K) is determined as 'the difference between the result (B_i) expected at the moment of making the decision and the result (B_{i+t}) obtained after the implementation of the decision'. [5]

$$K= B_i – B_{i+t}$$

We can treat the definitions as comparable providing we measure the result of a decision in terms of its effectiveness on a scale from 0 to 1.

Risk is a term which is often used to determine the subjective attitude of a subject, organisation, or a system to the adverse effects or losses arising from possible events. In practice, this means that different subjects, organisations or systems will report different levels of risk in one and the same situation. However, risk assessment should be based on scientific and objective methods. This involves taking into account a number of internal and external factors, including the relationships with contractors, suppliers, workforce, as well as how dynamic the atmosphere in which a system functions is.

It is obvious from the brief overview of the nature of cyber security risk to an organisation that to assess risk it is necessary to take into account a number of random variables and their probability distribution. This type of task is always classified as one having great complexity due to the high level of uncertainty in verifying the result. Often, such tasks can only be solved using some specific interpretation of data or knowledge of the field in question.

Често пъти такива задачи могат да се решават само на основата на специфична интерпретация на данни или готови знания за конкретната предметна област.

As a result of this complexity, most organisations use one of the existing methodologies of cyber security risk assessment such as the risk assessment frameworks developed over the past few years. Some of the most commonly used risk assessment frameworks are NIST SP 800-53 Rev. 4 and ISO/IEC 27001:2013.

The descriptive framework CSF (Cybersecurity Framework) developed by NIST (National Institute of Standards and Technology) is used by government agencies, as well as by businesses and educational institutions. Applying it is an indication of quality cyber security risk management processes at an organisation.

The standardised framework comprises three elements - framework core, framework implementation tiers and framework profile [4]:

Framework Core: This is a set of cyber security activities, desired outcomes and applicable references which are common across critical infrastructure sectors. It allows for the communication of cyber security activities and outcomes from the executive to the operations level of an organisation. The framework core has five simultaneous and continuous functions: identify, protect, detection, response and recovery. They all include categories and subcategories. The IDENTIFY function has a subcategory Risk Assessment – Fig. 1.

They all include categories and subcategories [of cyber security activities]. [For example, one of the functions the framework core serves is] the IDENTIFY function. It groups these activities under

five categories. One of them is Risk Assessment (ID.RA). The activities which go under the six subcategories of Risk Assessment all aim to help the organisation understand the cyber security risk to its operations. These involve identifying and documenting asset vulnerabilities (ID.RA-1), receiving threat and vulnerability information from information sharing forums and sources (ID.RA-2), identifying and documenting threats (ID.RA-3), identifying potential business impacts and likelihoods (ID.RA-4), using threats, vulnerabilities, impacts and likelihoods to determine risk (ID.RA-5), identifying and prioritising risk responses (ID.RA-6). Each subcategory is matched with relevant references such as existing industry standards, guidelines and practices – Fig. 1

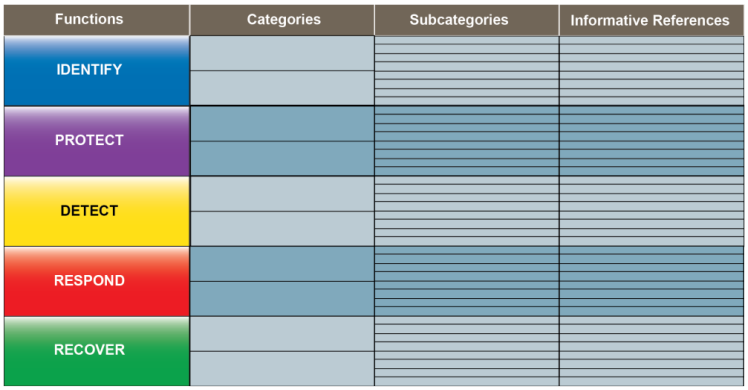

Fig.1 Framework Core.

Framework Implementation Tiers: This part provides information on how an organisation perceives the relevant cyber security risk and the processes in place to manage that risk. According to the degrees of implementation of risk management practices, organisations are partially aware of risks (Partial - Tier 1), informed of the existing risk (Risk Informed - Tier 2), constantly reassessing risk (Repeatable - Tier 3), and organisations adapting to the changes in the registered levels of risk (Adaptive Tier 4).

Framework Profile ("Profile"): A Profile is a specific description of the functions, categories and subcategories relevant to an organisation. It allows an organisation to 'take a picture' of its cyber security system. Using its profile an organisation can determine its present state, its desired state, and can map out the route to its goal. The profile is also recommended to organisations which need to interact and are trying to harmonise their profiles for better communication.

As for the methodology of assessing cyber security risk, as already mentioned, the process is described under the IDENTIFY function and the Risk Assessment category (NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16). The activities which go into assessing risk and the way to measure it are determined under this subcategory (Risk assessment - RA-3), in only three paragraphs as follows:

- Risk assessment takes into account the potential damage caused by gaining unauthorised access to or by using, disclosing, interrupting, changing or destroying the information system or the information processed, stored or exchanged;
- Risk assessment takes into account the likelihood of threats, the degree of vulnerability and the risk external to the organisation;
- Risk assessment takes into account (formal or informal) can be carried out at all three levels of risk management (at orginisation level, at mission / business process level and at information system level)

Another framework widely used to determine the cyber security system is ISO/IEC 27001:2013. In fact, the ISO/IEC 27000 series was jointly published by the International Standardisation Organisation (ISO) and the International Electrotechnical Commition (IEC). Similarly to the NIST frameworks, those of ISO are flexible enough to match most organisational requirements and structures. The frameworks encourage organisations to assess their own IT security risks and to

exercise control according to their needs. The ISO series also encourages feedback as a way to cope with the changes in the external or internal threats and implement iterative improvements.

ISO/IEC 27001 formally determines the absolute requirements which an information security management system (ISMS) should meet. It uses the ISO/IEC 27002 standard as a suitable information security control measure within the risk management system. However, since ISO/IEC 27002 is just a code of practice, or a guideline, not a certification standard, organisations are free to choose and implement other control measures, as well as additional information security controls, as they see fit. ISO/IEC 27001 includes an overview of ISO/IEC 27002 controls in Appendix A. In practice, most organisations which implement ISO/IEC 27001 also implement ISO/IEC 27002.

In this standard cyber security risk assessment is treated in the ISO/IEC 27001:2013 A.12.6.1 chapter [6].

It is only two paragraphs, 6.1.2 (c) and 6.1.2 (d), which specify what is implied by risk assessment and how risk is measured. According to them risk assessment should be made in view of the realistic likelihood of

Това са: Оценките на риска да се извършват с реалистична вероятност от възникване на загуба на поверителност, цялостност и наличие на информация в обхвата на информационната система.

It is obvious that even the frameworks most widely used to describe cyber security systems do not specify the methodology of determining the random variables which take part in assessing risk. However, both frameworks describe the medium on the basis of general factors such as adverse impacts of an occurring threat, vulnerability, external risk, confidentiality, integrity and the availability of information.

In both frameworks, risk assessment is accompanied by a sufficiently comprehensive analysis of the medium, whereby the existing threats (internal and external) and their relation to the vulnerabilities of the information system (a relation to issues such as confidentiality, integrity and availability of information) should be clearly identified. The next step is to determine the potential adverse impact of a threat. The interaction of two random variables, threats and vulnerabilities, is obvious, and the result of this interaction can be defined as the value of risk.

One possible solution to the risk assessment task with the above-mentioned parametres is to use the theory of fuzzy sets, applying fuzzy logic to their interaction.

The logic should reflect the general value of cyber security risk, taking into account the elements ‘cyber threats’ and ‘resilience’ of the system to such threats (the level of threat and the level of resilience), i.e. their combined effect on the level of risk. Generally, this combined effect can be represented as a set of different states, the corresponding value of risk and the function which characterises this correspondence. Such a set of states (possible combined effects) is described as a fuzzy set, and operations with such sets are described as fuzzy logic. Therefore, the risk ($K_{general}$) can be represented as a combination of the fuzzy set which reflects the possible threats ($K_{cybertreats}$) and the fuzzy set which reflects the resilience of the cyber security system ($K_{resilience}$) (the level of vulnerability subtracted from 1):

$$k_{\text{cybertreats}} = \{\mu_{\kappa}(x)/x\},$$

$$k_{\text{resilience}} = \{\mu_{k}(y)/y\},$$

$$k_{\text{general}} = k_{\text{cybertreats}\kappa} \cup k_{\text{resilience}},$$

where $\mu_k(x)$ and $\mu_k(y)$ are the characteristic functions showing the relation between the relevant cyber threat value ‘x’ and resilience value ‘y’ to the respective risk quotient. The general quotient is the result of merging them. Therefore,

$$K_{general} = \max(\mu_k(x), \mu_k(y)) = \mu_k(x) \vee \mu_k(y).$$

The merging of the two fuzzy sets leads to their fuzzy logic interaction, represented in this case by disjunction. The practical solution to such a disjunctive logic can be based on a Mamdani algorithm.

To determine the general risk quotient using a Mamdani algorithm it is necessary to determine two basic elements: firstly, the rules of interaction between the two variables and, secondly, the fuzzy set characteristic functions.

In determining the rules of interaction it is good to represent the variables in the same format and measure units. This is not obligatory, but it makes it convenient to formulate rules and draw conclusions.

Possible sample solutions to the task:

Възможни примерни условия за решаване на задачата:

In describing the rules, for all of the variables used – risk, threats and resilience – we adopt three possible values: 'low', 'average' and 'high'.

We use a variables interaction rules logic shown in Solutions Table 1.

Table 1.

Cyber threats Resilience	low	average	high
high	low	average	average
average	average	average	average
low	high	high	high

Risk Level

Value range of variables (0 – 100).

Characteristic function – a double Gauss matrix,

$$f(x) = e^{-\frac{(x-C_1)^2}{\sigma_1^2}} - e^{-\frac{(x-C_2)^2}{\sigma_2^2}}.$$

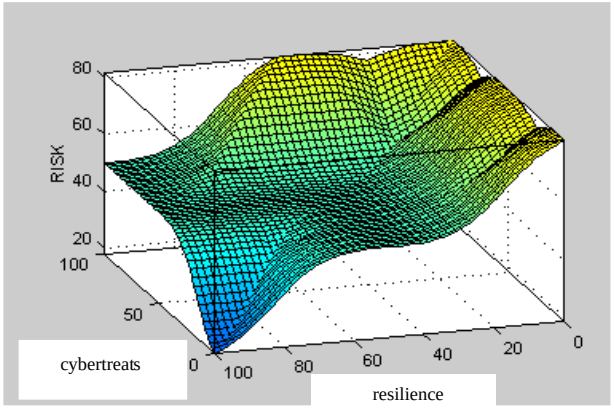

Fig.2 Result of the interaction between the variables 'risk', 'cyber threats' and 'resilience'.

The result of the fuzzy logic interaction which follows the determined rules is graphically represented in Figure 2. It is possible to distinguish clearly between three characteristic areas: two steep areas and a plain. In addition to the possibility of making a quick graphic (instrumental) analysis of the result, the approach represented above allows for a high-resolution formal risk assessment. The analysis makes it possible to apply this approach along with the above-mentioned frameworks, supplementing them without breaking the basic principles of description.

In conclusion, it is possible to say that the suggested solution could be improved by studying further different characteristic functions, changing the logic applied and, last but not least, verifying the results.

References:

1. https://mgimo.ru/upload/iblock/2d5/2d5686c9163ee863339211b841c8bf72.pdf - „Globalynaya bezopasnosty v tsifrovuyu эpohu: strategemы dlya Rossii" Pod obsht.red. Smirnova A.I. – M. : VNIIgeosistem, 2014
2. https://www.helpnetsecurity.com/2017/11/13/risk-assessment/

3. http://www.springer.com/gp/book/9789811000133 „Risk Analysis and Management: Engineering Resilience” - 2015
4. NIST SP 800-53 Rev. 4
5. Sapundzhiev „Vzemane na reshenie v sistemite za upravlenie” – TU 1998 g.
6. ISO/IEC 27001:2013