International Journal of Security and Its Applications
Vol.8, No.5 (2014), pp.21-30
http://dx.doi.org/10.14257/ijsia.2014.8.5.03

A Scenario-Based Information Security Risk Evaluation Method

Xiaofang Ban and Xin Tong

China Information Technology Security Evaluation Center
Beijing, China
tongxin2030@163.com

Abstract

Risk evaluation is the core process of information security risk management. An effective risk evaluation can protect organizations and maintain their abilities to carry out missions and activities against threats as well as helping to implement controls and safeguards that are actually needed. While the traditional information security risk evaluation approaches are lack of granular analysis and clear expression of security characteristics of risk, such as the possibility, attack path, and business impact. This paper presents the scenario-based information security risk evaluation method, based on the thought of Advanced Persistent Threat (APT) attack, by constructing risk scenario, evaluate information system security risk status. The separation analysis of the technical impact and business impact contribute to the technicians and business decision makers to grasp system risk status from their respective responsibilities. In the end of the paper, we propose a practical risk scenario construction example, which provides scientific and effective guidance for the preparation of a risk evaluation report.

Keywords: *risk evaluation, risk scenario, business impact, vulnerabilities, asset value chain, risk integration*

1. Introduction

In recent years, systems are becoming more susceptible to these threats due to the increasing interconnectivity of computer networks and more interdependent and accessible to a large number of individuals. The concern and interest in information security is mainly due to the fact that information security risk evaluation is a vital method to not only to identify and prioritize information assets but also to identify and monitor the specific threats that an organization induces; especially the chances of these threats occurring and their impact on the respective businesses. Therefore, information security risk evaluation plays a crucial role, which is applied to the entire life cycle of information systems. It is an essential technical mean to help organizations to determine the risks within an information system and provide sufficient means to reduce these risks.

Nowadays, there are a number of different types of risk evaluation methods and specifications that are available. Methodologies of risk evaluation generally fit into two categories: qualitative, quantitative and combination of the two approaches [1]. Qualitative risk evaluation methods are based on judgment, intuition, and experience, such as HAZOP, Fault Tree [2-5]. However, qualitative measures are subjective in nature. The major disadvantage of qualitative methods is its nature in producing subjective results which rely heavily on the quality of the risk evaluation team. In contrast, quantitative risk evaluation methods, using mathematical and statistical tools, attempt to assign specific numbers to the costs of safeguards and the amount of damage that can take place, such as Markov, Analytic

ISSN: 1738-9976 IJSIA

Hierarchy Process (AHP), attack graphs [6-10]. And While these methods lack of good quality data for estimating probabilities of occurrence or loss expectancies. They represent the risk results by quantify the risk with numerical number, while rather lack granular analysis and clear expression of causes, possibility, attack path, and the business impact of risk, so that the evaluated organizations are unable to accurately grasp the severity of their risks.

Meanwhile, in risk impact analysis, confusions are often made between technical impact and business impact caused by the information security incidents. Moreover, it is also lack of effective analysis of attack pathway due to the risks' combination. To solve the disadvantages of the above risk evaluation methods, this paper puts forward a scenario-based information security risk evaluation method, which evaluates the information system security status by constructing risk scenarios, from the angle of simulating attacks. This paper defines the evaluation process, the scenario construction factors, the risk integration steps and the risk scenario description of the scenario-based information security risk evaluation method. Scenarios can be represented in various ways [11, 12]. The concepts used in the process are well defined and the activities and steps of the process are also well explained. This allows better adoption to a methodology's concepts and notations and therefore better integration within the expression of risk evaluation results. In the end of this paper, it also gives a more practical example of constructing risk scenarios, which will provide guidance for writing a risk evaluation report.

The remainder of this paper is organized as follows: in Section 2, the normal process of scenario-based information security risk evaluation method is presented. Section 3 discusses the factors of constructing the risk scenario. A scenario constructing example is provided which is corresponding to the presented method, in order to show how to express evaluation results accurately in Section 5. In Section 6, we summarize our work.

2. Scenario-based Information Security Risk Evaluation Method

The scenario-based information security risk evaluation method is based on the identification of information asset, and then analyzes vulnerabilities and their severities. It constructs the risk scenarios for the high-level vulnerabilities, analyzes the occurrence possibility of each risk, and finally makes decision of its technical risk and business risk. The risk evaluation process is shown in Figure 1:

Step 1: Identify the key assets of the information system. See the assets classification in ISO/IEC 27005.

Step 2: Identify the security vulnerabilities of information systems. Including technical vulnerabilities and manage vulnerabilities.

Step 3: Determine the severity of the vulnerability. If the vulnerability level is low, then let it be the risk reference object; if the vulnerability level is high, and then build the risk scenario.

Step 4: Construct risk scenarios. See section 3 in this paper.

Step 5: Evaluate the risk occurrence possibility.

Step 6: Evaluate the impact caused by risks, including the technical impact and business impact.

Step 7: Determine the technical risk level and business risk level of the scenario.

Step 8: Determine the overall risk level of the information system. Let the highest risk level of the business risk be the ultimate risk level.

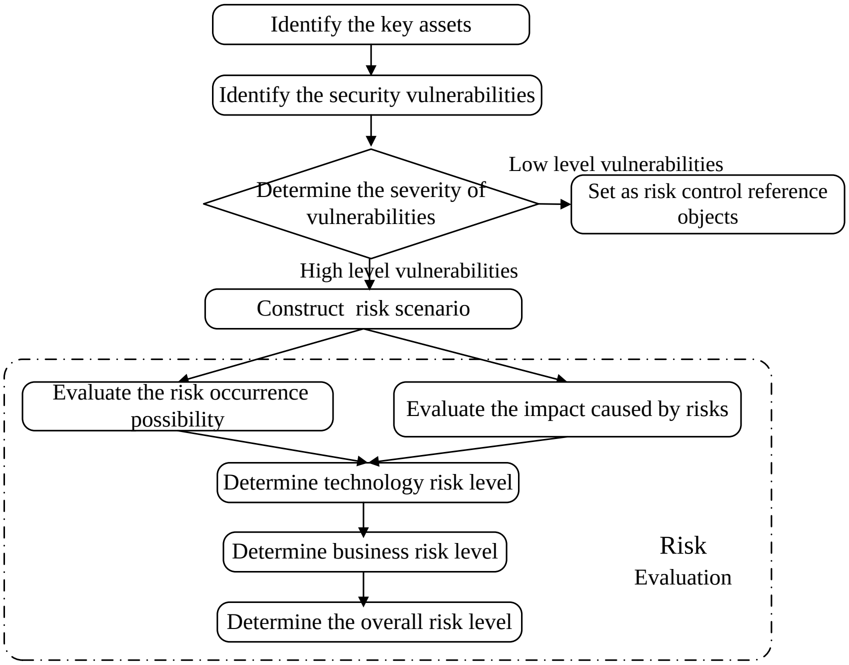
Identify the key assets
Identify the security vulnerabilities
Determine the severity of vulnerabilities
Low level vulnerabilities
Set as risk control reference objects
High level vulnerabilities
Construct risk scenario
Evaluate the risk occurrence possibility
Evaluate the impact caused by risks
Determine technology risk level
Determine business risk level
Determine the overall risk level
Risk Evaluation

Figure 1. Process of Scenario-based Information Security Risk Evaluation Method

Note that each information system risk scenario is constructed based on the high-level vulnerability. Due to the relevance of risk and vulnerability, the risk of low-level vulnerabilities is relatively low, thus for the low-level vulnerabilities do not construct risk scenarios. In addition, there is no one-to-one correspondence between the scenarios and vulnerabilities, there will be the situation that multiple vulnerabilities combining together to construct one scenario, while a single vulnerability can construct one risk scenario at most.

Compared with the traditional risk evaluation methods, the scenario-based information security risk evaluation method has been improved in the following areas:

1. Highlight the key risk. The construction of risk scenarios is based on vulnerabilities rather than on the assets. The existing security risk evaluation methods have correspondence analysis on assets, threats, and the vulnerabilities, they try to exhaust all the security incidents, while the evaluated organizations cannot grasp the main risk quickly.
2. Separate the analysis of technical impact and business impact, highlight the business risk analysis. In risk impact analysis, this method considers not only the technical impact but also the business impact. The business impact analysis considers the value of information assets. Considering the different business missions of information systems, there will be the case that technical risk level is high, while because its business is relatively not very important, the business risk level is not high. By separating the analysis of technical impact and business impact, it is helpful for the technicians and business decision makers to master system risk status from their respective responsibilities, while the traditional information security risk evaluation methods don't distinguish the difference.
3. Provide the overall information system risk decision method. The risk evaluation results can not only show the risks ranking, but also give the overall risk evaluation conclusions. It is helpful for the horizontal comparison of different risk evaluation

conclusions in a wide range. This method can measure information security risk distributions of multiple information systems in one organization.

3. Factors of Constructing the Risk Scenario

Constructing risk scenarios is the core of scenario-based information security risk evaluation method. It contains at least the following factors:

3.1 Time Factor

Time factor is the time when risk scenario occurs. If the information systems security is divided into three states, namely, past, present and future. The time factor can evaluate whether the information system has been attacked in the past, whether it is suffering attack now, and what kinds of risks it will face in the future. The description of the scenarios occurrence time contributes to an overall evaluation of information system security status.

3.2 Location Factor

Location factor is where the risk scenario occurs. It can be divided into physical location and logical location. Physical location refers to the physical environment, such as the city, building, or computer room; logical location refers to logical environment, such as the network, DMZ zone, or IP. The description of scenario location factor can make clear the origin position and the preliminary scope. It is also helpful for fast positioning at the risk disposal so as to determine the impact diffusion.

3.3 Threat Source Factor

Threat source factor is that the inducements for risk scenarios, including personnel, viruses, and the natural environment. Personnel can be divided into internal and external personnel. Internal personnel refer to the internal management personnel, operation personnel, maintenance personnel and developers. External personnel are those who are not of the unit or some malicious attackers. The description of the threat source factors contributes to identify the risk causes in risk management.

3.4 Threat Means Factor

Threat means factor is the means used in the risk scenarios, which can be divided into intentional and unintentional means. Intentional threats include password attacks, impersonation, exploits, denial of service, social engineering and so on. Unintentional threats include misuse, abuse of authority operation, equipment aging and so on. The description of the threat factors can help the evaluated master the generating process of risk.

3.5 Vulnerability Factor

Vulnerability factor is the internal vulnerabilities that cause risk scenarios, including technical vulnerabilities and management vulnerabilities. Vulnerability factor is the internal cause of the security risk and is the core risk in scenario construction. A risk scenario could be caused by a single vulnerability or by multiple vulnerabilities in the attack path.

3.6 Possibility Factor

Possibility factor is that the probability of the scenario. The possibility factor is closely related to the threat source and the threat motivation. For example, to evaluate the intentional threat possibility, we will focus on the attacker's skill and experience, tools and equipment requirements, attack time costs, the network location. While the unintentional threats possibilities typically include internal personnel, concerned about their business proficiency, work grievances, and operating authority.

3.7 Impact Factor

The impact factor refers to the possible impact on the risk scenarios, which also can be divided into technical impact and business impact. Technical impact refers to the direct impacts on confidentiality, security, availability. Business impact is the indirect impacts on business mission, corporate reputation, strategic development that the risks support.

4. Method for Information Security Risk Integration

Most of the information system security risk is caused by an attacker using a combination of multiple vulnerabilities. Therefore, in the construction risk scenarios, how to integrate single risk scenarios is the key to the scenario-based information security risk evaluation method. The ideas of risk integration come from the popular large-scale combinatorial attack, and its core is to analyze security vulnerabilities associated with the combination to form more comprehensive risk scenarios from an attacker's point of view. Risk integration is the process that simulate the intruders to "expand the record", and its nature is to study the spread and the transmission relationship of the information security risks.

In this paper, taking a group company with a number of subsidiaries as an example, we analyze risk transfer relationship, based on outlining the information assets value chain. Assume that the group company has headquarters and subsidiaries, as shown in Figure 2. At the industry's overall level, data interaction are staggered horizontally and vertically, namely headquarters decision information system and subsidiaries information system have vertical data exchange, and there are transverse data exchanges between information system of subsidiaries. At the institutional level, multiple information systems support its business operation, the core information systems and other information systems exchange data, information systems rely on each other. At the information system level, information system components including hardware, software and the environment are mutually dependent.

If there is a problem in a part of the information system, due to the value dependence of information assets, it will pass along the asset value chain and amplified. Meanwhile, the complexity of network and the support capacity of IT infrastructure make information security risks show a spread trend outside the assets value chain, resulting in the information security risk transfer impact more complex. Therefore, the information security risk integration process requires scientific guidance.

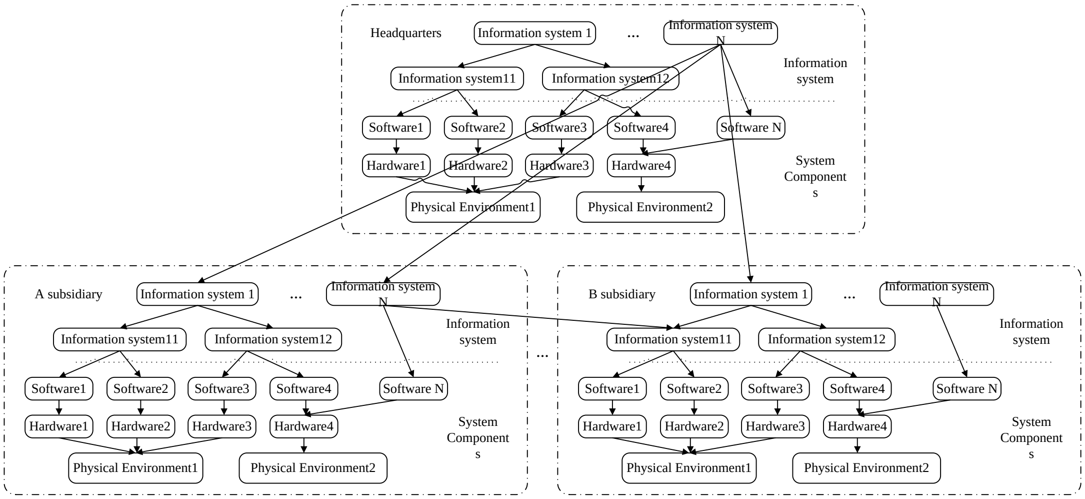

Figure 2. Schematic Diagram of Industry Information Assets Value Chain

Before risk integration, we should first build a single risk scenario and classify the risk scenarios. The risk scenario classification method has related with the target, content and preference of risk evaluation, which is facilitate to determine the association between scenarios in the next step. For example, based on the risk impact scope, the risk scenarios can be divided into system level, institution level and industry level; based on the information system components, the risk scenarios can be divided into physical environment, network, host, application, data, management and terminal; based on security characteristics, risk scenarios can be divided into security policy, security protection, security detection, security response, safe recovery; based on security influence receptors, the risk scenarios can be divided into individual impact, companies impact, social impact and national security impact scenarios and so on.

In the construction of complete single risk scenarios, we study the interdependence and interaction between risk scenarios, analyze whether associated risk can prompt higher threat occurrence possibility, or can cause greater harm to the information systems. If so, we construct new risk scenarios.

Information security risks integration includes the risk scenarios integration between similar system components, risk scenarios integration between system components, risk scenarios integration between information systems, and the inter-institution risk scenarios integration.

4.1. Risk Scenarios Integration between Similar System Components

System components are that constitute the information system, including computer room, networks, hosts, applications, data, management, terminals, personnel and so on. Risk scenario integration between similar systems components mainly focus on the risk transfer relationship between different risk scenarios with the same category components in the information system.

Case: Suppose machine “A” and machine “B” each have account “a” and account “b”, and establish accounts’ relationship of mutual collaboration and trust. That is, login with account “a” on machine “A”, you can unimpeded remote machine B, which is equivalent to account “b” privileges on the machine “B”, this is the host class risk scenario AA. Meanwhile, it is found that the authentication of account “a” has a weak password. This is the scenario BB which belongs to the host category as scenario AA. Thus, the risks of scenario AA and scenario BB can be integrated, so we get associated risk scenario CC. The event is that the external threats use the weak authentication password login account “a”, via the remote invocation, execute account “b” permissions on machine “B”. The impact scope of scenario CC includes machines “A” and “B”, which is more severe than the impact of scenario AA and BB on a single host.

4.2. Risk Scenarios Integration between System Components

Risk scenarios integration between systems’ components mainly focus on the risk transfer relationship between the components in the same information system.

Case: Suppose safety control measures have not been set in physical room, such as monitoring and limit host operation, so that external personnel can login any host within the computer room, this is risk scenario AA in physics class. Suppose host “A” has no password, but due to the separation of its network, and host “A” does not allow be remote operated, this is the risk scenario BB that constitutes a minimal effect in host class. By risk integration, scenario AA and BB can be associated obtained the scenario CC. The event is that the external personnel into the computer room, through login host “A” without password to access sensitive data. The impact of the scenario CC is more serious.

4.3. Risk Scenarios Integration between Information Systems

Risk scenarios integration between information systems mainly focus on the risk transfer relationship between multiple internal information system risk scenarios in one subsidiary.

Case: Suppose a business system data is changed after been invaded, which affects the subsidiary’s normal work. Because the system data is required real-time transfer to the core accounting system, it will cause corporate accounts confusion, and will do serious harm to the normal business operations. This is the information system risk transfer scenario after value-chain analysis.

4.4. Inter-Institution Risk Scenarios Integration

The integration of inter-institution risk mainly focus on transfer relationship of the business value chain among subsidiaries.

Case: Suppose the headquarters core network equipment breakdown, which will cause business pause, office disorder. Due to the information systems of the subsidiaries require real-time data exchange with that of the headquarters, if more than one information systems in headquarters stop running, it will affect the business of subsidiaries, resulting in the industry's overall business nearly paralyze.

The above four categories of risk integration are according to the asset size from small to large, respectively integrate new risk scenario with the risk of component level, system level, institution level, and industry level as an analysis unit.

5. Risk Scenario Constructing Example

A very important work in risk evaluation is how to express evaluation results accurately, on the base of accurate and scientific testing and evaluating, so that the evaluator and the owner can reach an agreement on the understanding of the final evaluation result. Therefore, this paper proposes a specific scenario constructing example corresponding to the scenario-based information security risk evaluation method, as shown in Table 1.

Table 1. Example of Constructing Risk Scenario

Factors of constructing the scenario	**Formal description**	
Scenario name	The portal directory traversal vulnerability exploited	
Risk scenario Level	Technical risk level	High
	Business risk level	High
Occurrence location	External network / DMZ zone	
Sources of threat	External attackers	
Occurrence time	Now	
Used vulnerability	Technical vulnerabilities	Directory traversal and database download vulnerabilities
	Management vulnerabilities	Null
Information assets	Physical assets	112.225.10.106
	Logical assets	Publicity and display information
Scenario description	1. There is an IIS directory traversal vulnerability in the portal, so that the malicious attackers can download the database files; 2. By downloading the database file, he/she can crack the administrator password, and then login the management platform successfully; 3. He/She can upload a web shell, elevate privileges, and then obtain system privileges successfully; 4. This host as a “intrusion pathway”, so that an attacker can invade from the external network to the internal company network.	
Risk impact analysis	Technical impact	The network exists intrusion pathway, due to the application relevance and interoperability between the various enterprises within the network, the vulnerability will result in "the whole network lost", so that the external protective measures across the enterprises network tends to be "nullified." The associated systems and their important business data will also be exposed to the attacker.

	Business impact	The portal has the features of releasing news and publishing strategic development information. Portal tampered may damage the company's reputation.
Evidence	List the relevant evidence, including but not limited to: attack pictures, video, document number, signed interview records.	

6. Conclusions

The traditional information security risk evaluation methods are lack of clear expression and granular analysis. Therefore, obtaining a sufficient number of vulnerabilities and risk results is not straightforward. This paper presents a scenario-based information security risk evaluation method, which easily highlight the key risk and distinguish the impact between technology and business. It is helpful for both the business decision makers and technicians to understand the meaning of risk evaluation results accurately. For carrying out an industry's overall risk evaluation, a unified risk evaluation method is proposed. The scenario-based risk evaluation method is flexible to allow integration into a methodological framework. The guidelines and the structural processes of the methodology will allow the explicit definition of the applicability of the security risk evaluation process within the stages of the methodology.

The constructions of formal risk scenarios and the descriptions of risk factors provide a set of practical scenario description examples for risk evaluation practices.

Combining the thought of Advanced Persistent Threat (APT) attack, this paper proposes a risk integration method, which further expands the connotation and extension of information security risk. This method also solves the mapping and divergence relationship between the assets value chain and risk transmission chain. Currently, the risk evaluation methodology proposed in this paper has been applied to the risk evaluation practice. Practice shows that the security status of information system can be outlined more accurately by using this method.

Acknowledgements

We are grateful to Mr. Zhang Li, the director of information system risk evaluation department of China Information Technology Security Evaluation Center. His knowledge and support has led to innumerable improvements of this paper. Thanks are also due to a number of our colleagues who generously read the paper entirety and to give us the benefit of their tremendous suggestions. Each of them deserves credit for the quality and style of this paper.

References

[1] T. R. Peltier, “Information security risk analysis”, Auerbach Pub, **(2005)**.

[2] C. Albets, A. Dorofee, “Managing information security risks: The OCTAVE approach” Boston: Addison Wesley Inc **(2002).**

[3] L. Yongjing and W. Chuqiu, “Based on the Delphi method of deep excavation safety risk analysis”, International Conference on Artificial Intelligence and Education ICAIE, **(2010)** October, Hangzhou, China.

[4] G. Hongfang and Z. Xiangyang, “Studies of Risk Analysis Approach”, Computer Engineering, vol. 3, **(2001)**.

[5] F. Redmill, “Risk analysis-a subjective process”, Engineering Management Journal, vol. 2, no. 12, **(2002).**

[6] B. Littlewood, “A reliability Model for Systems with Markov Structure”, Applied Statistics, vol. 2, no. 24, **(1997)**.

[7] A. P. Moore, R. J. Ellison and R. C. Linger, “Attack Modeling for Information Survivability”, Technical Note CMU/SEI-2001-TN- 001, Carnegie Melon Univ. / Software Eng. Inst., **(2001)** March.

[8] R. Horsnell, “Role of venture capital in the UK electronics industry”, Science, Measurement and Technology, vol. 137, no. 6, **(1990),** pp. 361-364.

[9] T. L. Saaty, “The Analytic Hierarchy Process”, McGraw-Hill, New York, **(1980).**

[10] C. Phillips and L. P. Swiler, “A Graph-Based System for Network-Vulnerability Analysis”, Proc. New Security Paradigms Workshop, **(1998)** September, Virginia, USA.

[11] I. Ray and N. Poolsappasit, “Using Attack Trees to Identify Malicious Attacks from Authorized Insiders”, Proc. 10th European Symp. Research in Computer Security (ESORICS’05), **(2005)** September 12-14, Milan, Italy.

[12] J. Ryser and M. Glinz, “SCENT-a method employing scenarios to systematically derive test cases for system test”, Technical Report 2000.03, Institut für Informatik, University of Zurich, **(2000)**.

Authors

Ban Xiaofang, she is currently the vice director of system evaluation division of China Information Technology Security Evaluation Center. She received her BS degree in Computer Engineering from Chongqing University in 2005. She has very rich practical experience on information system security risk evaluation. Her scientific research direction: network security and information system risk evaluation.

Tong Xin, she received the Ph.D. degree in information security from Beijing University of Posts and Telecommunications University in 2008. She is associate researcher of system evaluation division of China Information Technology Security Evaluation Center. Her interests are information system risk evaluation and communication security.