A General Method of Risk Estimation

Conference Paper · September 2023

DOI: 10.1109/ACIT58437.2023.10275626

6 authors, including:

Tetiana Korobeinikova
Lviv Polytechnic National University
35 PUBLICATIONS **28** CITATIONS

SEE PROFILE

A general method of risk estimation

Tetiana Korobeinikova
Department of Information Technology Security
Lviv Polytechnic National University
Lviv, Ukraine
ORCID 0000-0003-2487-8742
tetiana.i.korobeinikova@lpnu.ua

Illia Tachenko
Department of Information Technology Security
Lviv Polytechnic National University
Lviv, Ukraine
ORCID 0000-0001-9726-5942

Roman Chekhmestruk
3D GENERATION UA LLC
Vinnytsia, Ukraine
rc.ua@3dgeneration.com

Pavlo Mykhaylov
CEO 3D GENERATION GmbH, Dortmund, Germany
pm@3dgeneration.com

Olexandr Romanyuk
Faculty of Information Technologies and Computer Engineering
Vinnytsia National Technical University
Vinnytsia, Ukraine
rom8591@gmail.com

Sergey Romanyuk
Department of Biomedical Engineering
Odessa National Polytechnic University
Odessa, Ukraine
romaniuk.s.o@op.edu.ua

***Abstract*—Each company has assets of various types. Assets are associated with the concept of risks, so there is a necessity to analyze and research them etc. This paper is devoted to a general risk estimation method, which is unlike analogs uses vulnerability matrix for separate risk estimation.**

security risks, method of risk estimation, risk estimation

I. Introduction

The modern world is constantly moving towards computerization, the number of active users and devices on the Internet is constantly growing [1]. So, the load on network security is increasing. In 2021, international organizations revealed that each of them had in average 26 security incidents, which is 20% more than in 2020. A lot of different aspects give more chances for hackers and various criminal organizations, so the number of security incidents will grow. In 2022, 64% of companies had security incidents. To regulate the security aspects, the standards, rules, and laws are used [2–5]. However, the method by which criminals pursue their goals remains the same. This method is finding vulnerabilities and exploiting them [6-7]. Therefore, such vulnerabilities must be found by the security team before being exploited [8]. These arguments are related to network security risks (NSR) processes and methods determining and estimation. That is why the research topic is *relevant*. The goal of the research is to enhance the company security level by means of general method of risk estimation.

Asset-based risk assessment is often considered superior to scenario-based approaches. However scenario-based risk assessment can be done quicker, it also heavily relies on professionalism of the assessor [9-10]. While asset-based risk assessment has more strict structure and has it's own algorithm. There are tools and platforms that can help with assessment: nTask, ARC Cyber Risk Management, StandardFusion, etc. However, those tools are similar to exel documents with some additional features like presets of ISO standarts. Anyway, they can definitely help you with the risk assessment, and speed it up a little.

II. Technological Chain Determining Network Security Risks

NSR estimation and management was established as a scientific field about 30-40 years ago. At the same time, conceptual principles, and methods for NSR estimation and management were developed [9-12]. These principles and methods are still fundamental for this direction [13-14], but literally within the last decade a lot of theoretical development and practical models and procedures have been invented. The technological chain determining NSR [16] contents: 1) Asset collection process [8]; 2) Asset list forming process (SOC and ISO [11-13]); 3) Asset analysis process; 4) Infrastructure analysis process; 5) Infrastructure benchmarking process; 6) Risk analysis and estimation; 7) creating recommendations process; 8) Implementation of controls process [11]; 9) Review and re-audit process.

Fig. 1 shows the technological chain determining network security risks [16].

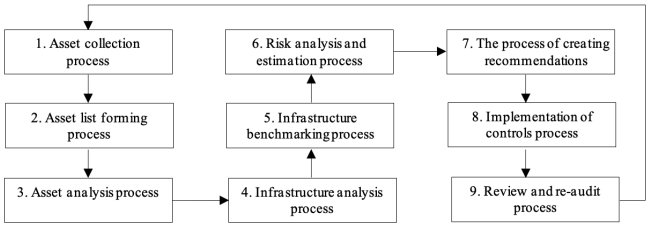

Fig. 1. Technological chain determining network security risks

III. Risk Analysis And Estimation Process

The process of risk analysis and estimation is our research interest within the scope of this paper. To approach this issue, it is necessary to define: basic concepts; concepts of critical assets.

A. Basic concepts

A critical asset (CAs) is an asset that is necessary for the company existence, and under the conditions of its destruction/disappearance, the company's work will be suspended. Signs of a CAs are: its high material value; the degree of importance for the existence/work of the company; difficulty or often impossibility of replacement (if it is possible to replace it – it is not critical).

CAs analysis – a process of determining the main functions and interaction of this CAs with other assets, determining the CAs impact on the integral work of the company's components.

CAs estimation – process of value displaying of an asset on different scales (tangible, intangible).

B. The concepts of critical assets

CAs are determined partly subjectively and partly using different techniques. Several criteria can be identified for determining CAs [16]:

1. The value and liquidity of the CAs itself (as a percentage of other assets);

2. Does the elimination of this component have any effect on the functioning of whole system (the number of hours the system can function without this component);
3. Does this CAs contain any information that should not be disclosed under any circumstances (the amount of funds that will be lost due to reputational losses and claims from the client).

CAs that are needed to support the business needs of both the local and national economy. These assets will have high failure consequences, but not necessarily high failure probability. CAs should be identified separately and estimated in more detail as part of the asset analysis process (item 3, fig.1).

Critical asset detection targets and refines actions, maintenance plans and financial plans in the most important areas. CAs may also include access to assets owned by third parties.

Let us show the way to identify CAs:

1. Identify and prioritize CAs based on privacy.
2. These are systems where unauthorized disclosure of data/information would have a serious impact on a company, such as:

- Systems containing customer's or employee's personal information where unauthorized disclosure could result any risk or negative consequences for these important groups (consequences include fines, significant direct recovery costs, and reputation loss);
- Previously published financial information that may lead to insider trading (consequences: criminal, regulatory, reputational);
- For companies that invest heavily in research and development, there may be a significant risk of unauthorized disclosure of proprietary intellectual property and/or trade secrets (company may even lose some legal protection if it doesn't remain trade secrets).

3. Integrity-based prioritization of CAs includes systems where the data alteration or corruption could have a serious impact:

- Financial systems, including banking or electronic funds transfers, where a change in data could lead to financial fraud/loss;
- Systems supporting regulatory processes where data loss or corruption could cause significant regulatory fines or other consequences.

4. Identify and prioritize CAs based on availability. These are systems that are considered critical when the company would be severely impacted if such systems were unavailable, for example:

- Industrial automation control systems (IAC – Infrastructure As a Code) used in critical infrastructures, such as electrical networks or pipelines;
- Medical technology systems used in modern health care system are closely related to IAC.
- Financial/ERP systems (ERP – Enterprise resource planning) needed to manage and maintain business cash flows;
- Core components of the IT infrastructure that are critical to other systems (Active Directory).

IV. A General Method Of Risk Estimation

Fig. 2 shows a scheme of general method of risk estimation.

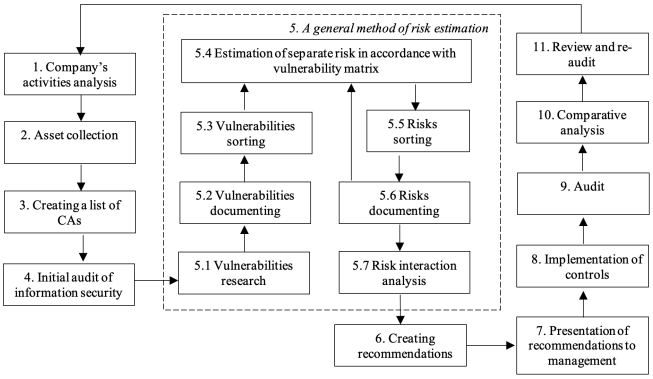

Fig. 2. A general method of risk estimation

Step 1. At the initial stage, it is necessary to determine company's nature and its activity.

Step 2. Determination of the general list of assets.

Step 3. Identification of CAs from the general list of assets and granting them a separate status.

Step 4. After that, it is necessary to provide an initial audit of company security level and define possible risks for each asset. A good solution is to choose 4 main risks for each asset.

Step 5. A general method of risk estimation. Vulnerabilities research, documenting and sorting used to estimate the separate risk in accordance with vulnerability matrix (tab. 1). The vulnerability matrix estimates separate risks and help to sort, document, and investigate how risks interact with each other.

Step 6. Making recommendations how to avoid/accept separate risks. If the risk is accepted, then estimate the amount of probable costs (losses).

Step 7. Making recommendations for assessing information security risks and proposing them to management. Thus, an initial audit in which the auditor's recommendations were considered and implemented is presented. The difference (in %) between the current company security level and the possible (desired) one is the degree of implementation of proposed recommendations.

Step 8. Implement controls that have been determined by management to be necessary.

Steps 9-11. After implementing the proposed recommendations, perform a re-audit of NSR and estimate the company security level using proposed method. Make a comparative analysis. If the predicted security level is less than the actual one, then the audit was done, but the risk estimation was not precise. This should be considered during the next risk estimation. If the predicted security level is greater than the actual one after a re-audit, then the plan is

recognized as incomplete. It is necessary to analyze reasons and considers during the next risk estimation.

A. How the vulnerability matrix which estimates separate risks works

Risk analysis – is a process that determines how likely a risk is to occur in a project. Risk analysis examines the uncertainties of potential risks and how they would affect the project. Two methods of risk estimation are quantitative and qualitative. It is important to monitor risks in the project life cycle. Qualitative risk analysis is an estimation made by experts who use data from past projects and their experience to estimate the impact and probability value for each risk on vulnerability matrix. The scale is from 1 to 5, where 5 is the most impact on the project. Once risks are identified, a project team member becomes a risk owner. He/she is responsible for risk response planning and its implementation (tab. 1):

Step 1. Estimate the frequency of the incident.

Step 2. Estimate the damage that destruction of a separate asset can cause (scale from 1 to 5);

Step 3. The indicators are multiplied and compared with the vulnerability matrix (tab.1). That helps to learn which risks are more important, which of them must be fixed first, and which of them can wait.

TABLE I. THE VULNERABILITY MATRIX WHICH ESTIMATES SEPARATE RISKS

Frequency / Amount of damage that can be inflicted	1 – Very rare	2 – Rarely	3 – Maybe	4 – Very possible	5 – Most likely it will happen
5 – Critical	5	10	15	20	25
4 – High	4	8	12	16	20
3 – Average	3	6	9	12	15
2 – Small	2	4	6	8	10
1 – Insignificant	1	2	3	4	5

For example, theft of an employee's laptop. The frequency of such thefts is rare, but if this laptop had any important data on it or saved passwords to systems that could stop the business, it could lead to large losses. That is, the frequency is 2, the amount of damage is 4. The product of these numbers is 8. This means that the indicated risk is orange one, which is one of the four risk types: green – the risk is insignificant and most likely will not happen; yellow – the risk is not too high, or the probability that it will happen is very low; orange – the risk is high and needs to be addressed if there are no critical risks; red – the risk is critical and needs to be addressed immediately.

B. Scheme of assessment and analysis of a separate risk

The scheme of assessment and analysis of a separate risk is shown on Fig. 3.

Step 1. Using the data from the comparing infrastructure to standards process – it is Infrastructure benchmarking process from the Technological chain determining NSR (fig. 1), the gaps in information security are found and highlighted. Put the gaps into a separate document. Remark 1: Example. "The company does not have EDR (Endpoint detection and Response), MDM (Mobile Device Management tool), processes for checking employees for criminal records, and cameras at the entrance."

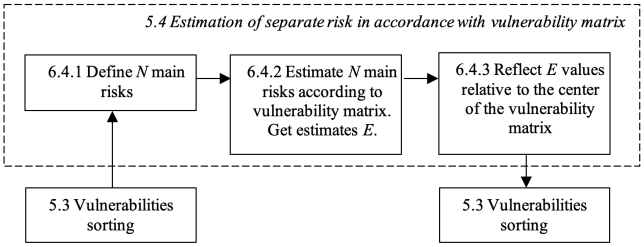

Fig. 3. Scheme of separate risk estimation in accordance with vulnerability matrix

Step 2. Sort the vulnerabilities by groups, relative to parts of the infrastructure (item 5.3 on fig. 3). Remark 2: Many frameworks have their own groups for risk estimation (CISv8, 1.3.3) [15-17]. In given example, there are 2 gaps in Endpoint Security, 1 in Human Resources, and 1 in Physical security.

Step 3. The process of separate risk estimation in accordance with vulnerability matrix begins. The N main risks are defined (item 6.4.1 on fig. 3).

Step 4. The N main risks according to vulnerability matrix (tab. 1) are estimated and there are estimates E for each of these N risks (item 6.4.2 on fig. 3).

Step 5. Reflect E values relative to the center of the vulnerability matrix (item 6.4.3 on fig. 3).

Step 6. The estimation E values according to the number of risks and their value are grouped (vulnerability sorting, item 5.3 on fig. 3). Remark 3: Usually all document and steps are evaluated. After separate risk estimation, the risks interactions are analyzed (item 5.7 on fig. 2). In example, MDM and EDR are absent, so if some activity happens, it isn't blocked. These two combined risks become critical.

V. IMPLEMENTATION

The implementation of a general method of risk estimation at the VaultTech enterprise took place on 05.26.2022 (two letters in the company's name have been changed for security reasons and non-disclosure the enterprise official name). The implementation was applied in the Technical Innovations Branch and controlled by the Head of the Information Security Department.

As a result, criteria were found, to compare audit before and after the implementation of given method (tab. 2).

TABLE II. COMPARATIVE AUDIT BEFORE AND AFTER THE IMPLEMENTATION OF GIVEN METHOD

Criteria / Expert opinion	Before (0-10)	After (0-10)
Quick orientation in project	4	7
The number of vulnerabilities found	6	7
The number of assets found	7	8
Separate risk estimation	7	8
Using well-known standards	10	10
Quality of documentation	8	9
	42/60	49/60

This is result of the Information Security Department experts and CTO opinion. It was accepted that 0 points is a complete failure, and 10 is a perfectly done job. The difference is: 7 points, or 11.6%.

4. CONCLUSIONS

Technological chain determining network security risks consists of nine basic processes: asset collection process, asset list forming process, asset analysis process, infrastructure analysis process, infrastructure benchmarking process, risk analysis and estimation process, the process of creating recommendations, implementation of controls process, review and re-audit process. This technological chain, unlike similar ones, contains detailed and in-depth instructions of risk analysis and estimation process. Risk analysis and estimation process makes it possible to assess risks via using general method of risk estimation, which explains how offered vulnerability matrix estimates every risk separately. The vulnerability matrix estimates every separate risk by the frequency this risk occurs and the amount of damage that can be inflicted.

The detailed scheme of separate risk assessment is shown and descripted. In order to offered technological chain, the algorithm for determining network security risks is shown and descripted.

The main difference between the offered general method of risk estimation and existing approaches lies in the incorporation of two key features: a point-based safety level calculation and a correlation between different risks are based on infrastructure. These differentiating factors set offered method apart from traditional approaches and offer unique advantages in the risk assessment process.

The point-based safety level calculation provides a more granular and precise assessment of safety. Instead of relying on qualitative measures or broad categories, a general method of risk estimation assigns specific point values to different safety levels. This enables a more accurate quantification of safety and facilitates better decision-making in risk mitigation strategies.

A general method of risk estimation introduces a correlation between different risks based on infrastructure. By considering the interdependencies and interactions between various risks, a comprehensive understanding of combined impact is gained. This correlation analysis allows to identify potential cascading effects, evaluate systemic risks, and prioritize mitigation efforts accordingly.

These distinct features differentiate the general method of risk estimation from existing approaches, such as the globally widespread standard "ISO/IEC 27005:2022 Information security, cybersecurity, and privacy protection – Guidance on managing information security risks." While ISO/IEC 27005 provides valuable guidance, this method offers advancements in safety level calculation and the consideration of risk correlations specific to infrastructure. These enhancements contribute to more accurate risk assessments, better-informed decision-making, and enhanced risk management strategies.

As a result of implementation of a general method of risk estimation, the following criteria were identified: the possibility of quick orientation in project, the number of vulnerabilities found, the number of assets found, separate risk estimation, using well-known standards, quality of documentation.

The implementation of a general method of risk estimation enhances the company security level on 11.6% comparing with common approaches.

REFERENCES

[1] Korobeinikova, T., Maidaniuk, V., Romanyuk, O., Chekhmestruk, R., Romanyuk, O., & Romanyuk, S. (2022). Web-applications fault tolerance and autoscaling provided by the combined method of databases scaling. Paper presented at the 2022 12th International Conference on Advanced Computer Information Technologies, ACIT 2022, 27-32. doi:10.1109/ACIT54803.2022.9913098.

[2] Ukraine – Data Protection Overview, 2021. URL: https://www.dataguidance.com/notes/ukraine-data-protection-overview.

[3] Convention for the Protection of Individuals regarding Automatic Processing of Personal Data. Amendment to Convention ETS №108 allowing the European Communities to accede. URL: http://ippi.org.ua/sites/default/files/conv108.pdf.

[4] Law of the Verkhovna Rada of Ukraine On Protection of Personal Data, 2022. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

[5] The procedure for monitoring compliance with the legislation on the protection of personal data by the Commissioner for Human Rights of the Verkhovna Rada of Ukraine, approved by the order of the Commissioner for Human Rights of the Verkhovna Rada of Ukraine, 01/08/2014 № 1/02-14. URL: https://www.ombudsman.gov.ua/uk/kontrol-za-doderzhannyam-vimog-zakonodavstva-zpd.

[6] Shi, J. «Security risk assessment about enterprise networks on the base of simulated attacks». Paper presented at the Procedia Engineering, 24 272-277. doi:10.1016/j.proeng.2011.11.2640.

[7] What good AI cyber security software looks like in 2022. URL: https://www.itproportal.com/features/the-eu-gdpr-what-does-it-mean-for-application-security/.

[8] Wales E. Vulnerability assessment tools. Network Security, 2009,(7):15−17.

[9] Jbair, M., Ahmad, B., Maple, C., & Harrison, R. (2022). Threat modelling for industrial cyber physical systems in the era of smart manufacturing. Computers in Industry, 137 doi:10.1016/j.compind.2022.103611.

[10] Yunizal, E., Santoso, J., & Surendro, K. (2022). Asset identification in information security risk assessment using process mining. International Journal on Advanced Science, Engineering and Information Technology, 12(4), 1387-1394. doi:10.18517/ijaseit.12.4.14865.

[11] ISO 27001 Requirements – Information Security Management // Sprinto, 2021. URL: https://sprinto.com/blog/iso-27001-requirements/.

[12] ISO/IEC 27701:2019 Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines // International Organization for Standardization. 2022. URL: https://www.iso.org/standard /71670.html.

[13] ISO/IEC 27005:2022 Information security, cybersecurity, and privacy protection — Guidance on managing information security risks // Organization for Standardization. 2023. URL: https://www.iso.org/standard/80585.html.

[14] What is SOC 2. URL: https://socreports.com/audit-overview/what-is-soc-2.

[15] What is MDM // Zoho Corp, 2021. URL: https://www.manageengine.com/mobile-device-management/what-is-mdm.html.

[16] I. Tachenko, T. Korobeinikova, S. Zakharchenko, Overview of the current state of the issue in the field of network security risk assessment, in: Proceedings of the 5th International Scientific and Practical Conference «Theory and Practice of Science: Key Aspects» (November 7-8, 2021). Rome, Italy: Dana, 2021, pp. 417-432. doi: 10.51582/interconf.7-8.11.2021.

[17] CIS Critical Security Controls Version 8, 2021. URL: https://www.cisecurity.org/controls/v8.