https://doi.org/10.53656/isct-2025.22

Telecommunications and Signaling Equipment, Automation Systems in Transport

PROJECT-BASED APPROACH TO RISK MANAGEMENT OF TRANSPORT COMPANY INFORMATION SYSTEMS

Mario Bogdanović, Deni Vale
Istrian University of Applied Sciences, Pula, Croatia

Abstract. Information security, manifested as the protection of information and physical data carriers, is a fundamental element in ensuring the business success of transport companies. In order to maintain robust information security in terms of uninterrupted operational use, it is necessary to manage the risks of a given information system. This includes assessing and evaluating its most critical and high-risk components, as well as proposing alternative measures (strategies) for reducing risks (threats) and dealing with specific hazardous scenarios. This paper addresses the issue of achieving appropriate information security through risk management using a project-based methodology. The approach is presented through three defined problems and corresponding hypotheses: (1) Risk identification; (2) Risk quantification with categorization based on severity (high-level/kill risks, medium-level and low-level risks); (3) Determination of the suitability of various alternatives/strategies for managing all types and levels of risk. The results demonstrate that risks can be identified and quantified according to their severity in the information systems of transport companies. Risk mitigation can be approached through one of six (6) risk management strategies (risk avoidance, risk transfer, risk prevention, risk impact reduction, risk ignoring, contingency planning), through their combination/synergy, or by alternative means. The methodological principle of project management in the field of risk management has proven to be a suitable approach for managing risks in the information systems of transport companies and can also be applied to risk management in the information systems of other types of companies.

Keywords: information security; information system; risk management; risk management methodology; risk management strategies; transport companies

1. Introduction

Uncertainty and risk are inherent components of business life, and it is dangerous to ignore or deny their impact, as many things can go "wrong." Risk management is

particularly emphasized in project management, being one of the nine fundamental knowledge areas of the discipline itself [1]. It also draws on creative techniques that employ various modes of thinking to solve complex problems, with one of the key approaches being consideration of potential risks, dangers, damage, and the downsides of ill-considered decisions, which are known as the "black hat" in the Six Thinking Hats technique created by Edward de Bono (for example see Ref. [2]).

Potential threats, negative impacts, and harms arising from uncertainty are described using the terms uncertainty and negative risk. Uncertainty refers to a lack of information, knowledge, or understanding regarding the outcome of an action, decision, or event. Management often suffers from such a lack, which is crucial for effective decision-making. Risk is a measure of the degree of uncertainty and is directly related to the availability of information. The relationship between information and uncertainty is illustrated in Figure 1.

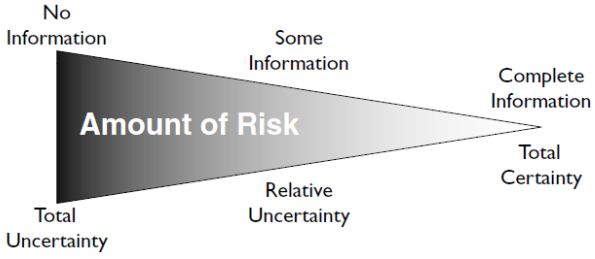

Figure 1. Risk relationship between information and uncertainty, taken from Ref [3]

Effective risk management requires the identification of threats, which are specific events that may lead a business system toward undesirable outcomes such as deadline overruns, cost overruns, poor quality, or failure to maintain business continuity. In digital business, risks arise from the intensive use of information systems and technology, which are essential for supporting and improving business processes and the overall functioning of any enterprise. Digital business risks depend on three variables: the assets of the business entity (both material and financial), threats (incidents, unwanted events), and vulnerabilities (system weaknesses resulting from poorly implemented control mechanisms), hence:

(1) $Risk = f(assets, threats, vulnerabilities)$

The manifestation of risk can be either direct or indirect and is typically reflected as a material or financial loss [4]. Material or financial loss occurs in relation to informational assets, which include everything that holds value for an organization, serves as information or contains it, and is used in service support processes based on that information [5]. According to Ref. [6], informational assets encompass

all resources that store, transmit, create, use information, or are information themselves.

Information systems of transport companies, regardless of the mode of transportation (automobile, bus, truck, rail, maritime, air, etc.), do not fundamentally differ from the information systems of other companies, as disruptions in these systems lead to similar or even greater negative consequences when security is compromised. In fact, if confusion arises within the information system, business operations and costs are quickly affected. For example, disruptions in timetables or the place/date of dispatch directly impact business efficiency. Therefore, every transport company should have a well-developed risk management scheme for each identified risk, with particular attention to those of higher magnitude.

2. Purpose, Objective, Problems, and Hypotheses of the Research

The purpose of this paper is to present a rational way (methodology) for improving information security in transport companies using a project risk management methodology. The main goal of the paper is to identify the most critical/riskiest parts of the transport company's information system and to propose measures/strategies for reducing certain fatal risks for these risks.

The problems of the work are defined as questions, hypotheses as hypothetical answers to the problems posed:

P1: What are the threatening risks for the information system of transport companies?

H1: It is possible to identify numerous risks of the information system of transport companies.

P2: Which risks of the information system of transport companies can be considered fatal risks (high-risk risks/risks in the high-risk zone), and which are medium and low-risk risks?

H2: It is possible to quantify kill risks (high-level risks) as well as medium and low-level risks.

P3: How to manage (which strategy) each of the quantified information system risks of kill (high), medium and low risk levels?

H3: It is possible to manage the identified and quantified risks using one of six (6) risk management strategies.

3. Research Methodology

For the first problem, the project risk identification methodology from Ref. [3] was used. Using the brainstorming/brainwriting method as well as thinking about potential risks/problems (answering the question: "What could go wrong?"), the risks of the information system were identified. Answers were offered with regard to experience, problems observed in information systems of other types of companies, and hypothetically possible threats.

The formula was used to solve the second problem, i.e. risk quantification:
(2)

$$R = probability\ of\ a\ risk\ event \times strength\ of\ the\ risk\ impact\ if\ it\ occurs.$$

The rating scale is 10 points for each element of the product (factor x factor). The results obtained are presented graphically for a clear representation of the risk zone (high, medium, low). The authors of the paper were the evaluators of each risk. The risk zones are presented in Fig. 2.

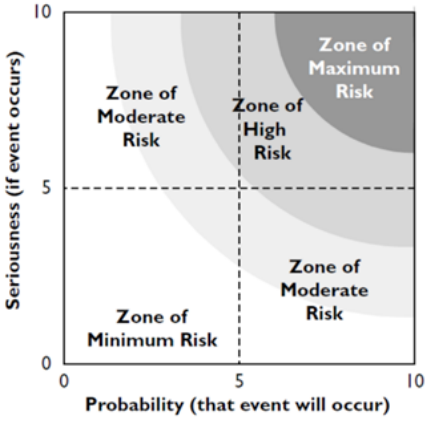

Figure 2. Identification of Risk Zones/Severity Levels, taken from Ref [3]

In the third problem, high (kill risks), medium and low level risks were linked to 6 different strategies. For those risks for which a suitable strategy could not be found, a new strategy, or alternative coping strategy, was proposed.

4. Research Results and Discussion

4.1. Identification and Quantification of Information System Risks in a Transport Company

The list of identified information system risks was obtained using the method of experience and creative production of the authors. A total of *N=44* risks were identified, which are also descriptively explained in an unpublished paper [7]. After identification, all of the listed risks were quantified. This was necessary to distinguish those risks that are high-level – the so-called high-threat/lethal risks – from those of medium and low-threat levels. The identified and quantified information system risks are presented in Table 1.

Table 1. Information system risks, their probability, impact strength and product (danger level)

Types of identified risk	Probability of risk occurrence	The strength of the risk impact if it occurs	Multiplier (danger level). 1=kill (70 – 100); 2=medium (40 – 69); 3=low (<39)
1. Theft of media and documents	4	8	32
2. Unauthorized changes to the system	6	9	54
3. Password security	8	9	72
4. Hacker attacks using specially crafted messages	9	9	81
5. Unauthorized entry into physical space	3	8	24
6. Interception of compromising interference signals	2	7	14
7. Interception of information/ espionage	4	9	36
8. Eavesdropping	5	8	40
9. Error in the application/use of the application	4	7	28
10. Data loss	8	9	72
11. Loss of integrity of sensitive information	1	9	9
12. Mismatched/incompatible IT equipment and resources	5	6	30
13. Electromagnetic interference	1	6	6
14. Flood/moisture/water	2	9	18
15. Fire/excessive temperature/ heat	2	10	20
16. Various natural disasters	1	10	10
17. Main event nearby	1	4	4
18. Failure or interruption of power supply networks/power outage	2	8	16
19. Denial of services (DoS)	5	7	35
20. Failure or interruption of communication networks	6	6	36
21. Coercion, blackmail or corruption	3	7	21
22. Identity theft	5	6	30

Types of identified risk	Probability of risk occurrence	The strength of the risk impact if it occurs	Multiplier (danger level). 1=kill (70 – 100); 2=medium (40 – 69); 3=low (<39)
23. Misuse of personal data	6	7	42
24. Malicious software	7	8	56
25. Denial of harmful actions (sabotage/damage)	4	7	28
26. Unauthorized use or management of devices and systems	6	7	42
27. Abuse of authority/privileges	5	8	40
28. Accidental loss of storage devices/media and documents	4	6	24
29. Sabotage/damage	3	8	24
30. Poor planning or lack of adaptation	4	5	20
31. Disclosure of sensitive information	3	8	24
32. Information or IT products from unreliable sources	3	7	21
33. Hardware or software manipulation	2	8	16
34. Information manipulation	3	7	21
35. Destruction of devices or storage media	2	9	18
36. Device or system failure/ malfunction	4	6	24
37. Pollution, dust, corrosion	3	6	18
38. Lack of financial resources	3	7	21
39. Lack of material and information/IT resources	3	6	18
40. Lack of human resources, i.e. staff / lack of trained personnel	5	7	28
41. Software vulnerability or errors	3	8	24
42. Violation of laws/regulations	2	9	18
43. Adverse climatic influences	2	9	18
44. Social engineering	3	6	18

4.2. Linking Risks with Response Strategies

The identified and quantified threats in the next step are linked to coping strategies, and the main way of implementation is shown in Table 2.

Table 2. Risk response strategies

Strategy	Low-risk threats	Medium-risk threats	High-risk threats
Ignore	Frequently applicable	Caution, only if the costs of protection are too high	Unacceptable, because the consequences could be great
Avoid	Almost not used	Sometimes, if there is an easier alternative	Useful when exposure can be avoided completely
Risk transfer	Rarely, unless already covered by insurance	Common practice (e.g. insurance, outsourcing)	Very common, especially through insurance
Prevention	Useful if it is cheap and simple	Recommended to reduce the likelihood	Mandatory, first line of defense
Impact reduction	If the consequences are known and tolerable	Often used in conjunction with prevention	Required in combination with other measures
Contingency planning	Rarely, unless it is part of a larger plan	Recommended – prepare for the worst-case scenario	Necessary – part of any serious security plan

Avoidance strategies for certain security risks in transport companies are sometimes possible but rarely fully feasible in daily operations. For example, switching to biometric authentication can reduce password-related risks, while spear phishing exposure can be limited through secure communication channels and email filters. However, in cases like data loss, avoidance is not an option due to the essential role of digital data processing in logistics, making prevention and contingency planning crucial. Ignoring risks is generally unjustifiable, and although risk transfer through insurance or outsourcing (e.g., cloud services, Managed Security Service Providers) can reduce the burden of consequences, while reputational and legal damages remain the company responsibility. Risk mitigation strategies for weak passwords include enforcing complex password policies, implementing multi-factor authentication, rotating credentials regularly, and using password managers with breach detection integration. For spear phishing attacks, effective strategies involve targeted staff training, secure email filtering, sender authentication protocols, and link/attachment sandboxing, supported by incident response and containment plans. In the case of data loss, the most robust strategy combines regular immutable backups (3-2-1 rule), access control based on user roles, offline storage, and predefined RTO/RPO parameters to enable rapid system recovery and maintain operational continuity. Here, we have briefly outlined only the strategies for high-risk threats, while a more detailed analysis, including strategies for medium-risk and low-risk threats, is presented in the unpublished study [7].

In this way, all identified and quantified risks are linked to coping strategies, which achieves significant progress in managing risks in information systems of

transport companies. Thus, the project approach has proven to be a good tool in managerial risk management of information systems.

Conclusion

Concisely summarizing the obtained results of this work, the following conclusions can be drawn:

P1/H1: Information systems of transport companies are exposed to numerous threats that include technical, organizational, human, legal and natural risks.

P2/H2: Based on a quantitative analysis of the probability of occurrence and the strength of the impact of each of the identified risks, it is possible to clearly distinguish the risks of the information system of transport companies according to their level of danger. The results shown in Table 1. confirm the hypothesis that it is possible to identify kill, medium and low-danger risks. Risks such as hacker attacks with specially crafted messages, password security and loss of business data are classified as fatal because they achieve high product values (above 70), which indicates their extreme harmfulness and high probability of occurrence. Most risks belong to the low-level category, most often due to low probability or limited impact. Such a categorization allows for the adoption of targeted and prioritized security measures, with an emphasis on proactive protection against high-level risks, thereby contributing to the resilience and continuity of information systems within the transport sector.

By linking the identified and quantified information system risks (P3/H3), it can be concluded that effective management of information system risks of fatal, medium and low levels of danger can be achieved by applying one or more of six risk management strategies, possibly their combination/synergy, where the choice of strategy depends on the type and nature of the individual risk. In situations where complete control over the risk is impossible or too expensive, a risk transfer strategy through insurance or contracts with external service providers may be an appropriate solution. Proper application of the strategy requires understanding the specific context and assessing the benefit-cost ratio for each individual risk. This confirms that all identified risks can be managed with a targeted strategy, thereby reducing their harmfulness and increasing the resilience of the information system of transport company.

Acknowledgement

Special thanks go to our colleague Marko Turk, MA Economics, lecturer at the Istrian University of Applied Sciences in Pula, Croatia, for his valuable assistance in compiling the data presented in Table 1. His professional and academic expertise in the field of information systems greatly contributed to the quality of this work, and we sincerely appreciate his support.

REFERENCES

[1] BUBLE, M., Projektni menadžment, Dugopolje (Croatia): Minerva University of Applied Sciences, 2010, 208 pp., ISBN 978-953-56361-0-6.
[2] DOMITRAN, I., Kako koristiti metodu „Šest šešira"? Poslovna učinkovitost d.o.o., 2014, available at: https://www.poslovnaucinkovitost.hr/kolumne/poslovanje/986-kako-koristiti-metodu-sest-sesira (accessed on 14 December 2021).
[3] HEERKENS, G., Project Management, New York, NY (USA): McGraw-Hill, 2002, 250 pp., DOI:10.1036/0071394494. The material in this Book appears as eBook 0-07-139449-4 and print version 0-07-137952-5.
[4] DALZIEL, H., Infosec Management Fundamentals, Amsterdam/Boston: Elsevier Science (Syngress), 2015, 72 pp., ISBN 978-0128041871.
[5] UREMOVIĆ, D., Kako upravljati IT rizicima. InfoTrend, 5 (2009), pp. 42 – 47, ISSN 1330-0393, available at: http://www.infotrend.hr/clanak/2009/6/kako-upravljati-it-rizicima,37,767.html (accessed 14 December 2021).
[6] HADJINA, N., Zaštita i sigurnost informacijskih sustava. Zagreb, Croatia: Faculty of Electrical Engineering and Computing (FER), University of Zagreb, 2009.
[7] BOGDANOVIĆ, M., VALE, D., A Detailed Project-Based Analysis of Information System Risks in the Transport Sector, unpublished manuscript, Croatia.

✉ **Prof. Dr. Mario Bogdanović, scientific adviser**
ORCID iD: 0000-0003-3049-5342
Department for Social Sciences
University of Applied Sciences in Pula
9D, Preradovićeva, Pula, Croatia
E-mail: mbogdanov@iv.hr

✉ **Deni Vale, mag. phys., lecturer**
ORCID iD: 0000-0002-3138-7581
Department for Technical Sciences
University of Applied Sciences in Pula
9D, Preradovićeva, Pula, Croatia
E-mail: dvale@iv.hr