Case study

STRATEGIES FOR MANAGING SECURITY RISKS IN POSTAL TRAFFIC: APPROACHES, CHALLENGES AND GUIDELINES

Binički, M.[1], **Kljak, T.**[2], **Škorput, P.**[2]

[1]Hrvatska pošta d.d., Zagreb, marijan.binicki@posta.hr
[2]University of Zagreb, Faculty of Traffic and Transport Sciences
tomislav.kljak@fpz.unizg.hr, pero.skorput@fpz.unizg.hr

Abstract: *The paper investigates the management of security risks within the postal system. The focus is on analysing security risks associated with key elements and processes in postal traffic, considering the likelihood of occurrence and the consequences of potential adverse events. The paper emphasizes that complete security and protection in a technical sense are neither achievable nor economical; therefore, it proposes the application of methods for risk balancing and control using the Trade-Off method. The use of the concept of risk-tolerant intensity in operational and security assessments is suggested. The paper systematizes security risks in terms of the potential for material or non-material damage due to the exploitation of system weaknesses by threats under certain circumstances.*

Keywords: *postal system, security risk, tolerable risk intensity, management*

1. INTRODUCTION

Familiarity with the general methodological approach to risk assessment according to the NIST method, ISO 2700X series standards, and similar recommendations for security risk management is crucial for understanding the specificities of risk assessment in the postal system (Kemp, 2021). The goal of risk assessment using the concept of Tolerable Risk Intensity and tolerance fields is to enable more realistic and effective decision-making regarding protection within the postal system and its immediate environment (Xueyan et al., 2019).

Creating and operationally verifying security measures for individual parts of the postal system provide a solid foundation for defining security policies, developing technical protection system projects, and significantly improving contractual relationships with customers and other postal process participants (Kowalik, 2020). Given the new forms of threats and dangers, it is necessary to redesign the existing approach and risk assessment methods, where the proposed solutions can be very useful (Xueyan et al., 2019).

Risk assessment is essential for successfully managing protection in postal traffic (Kemp, 2021). A quality and objective risk assessment in all phases and parts of the postal system requires the adaptation of technological processes and participant behavior. The distribution of responsibilities and authorities to achieve the desired level of protection includes active participation from all employees, which is difficult to achieve without specific methods and tools for security management (Fereirra, 2019).

Introducing efficient security devices to protect postal facilities, employees, and clients, as well as engaging security services, represents a fundamental strategic decision for management

(USPS, 2019). Detailed analysis of security risks and identification of security problems in different elements of the postal system are necessary for making informed decisions.

In the context of managing postal system security, it is important to improve protection methods using modern technical tools and technologies (Xueyan, 2019). This allows for achieving an acceptable level of risk with optimized costs. Assessments of the probability and consequences of harmful events enable the calculation of appropriate security indicators for all parts of the postal system.

2. SURVEY, ANALYSE OF RESULTS AND DISCUSSION

Preliminary research on the security of postal traffic included data and document collection, as well as conducting a survey among postal system employees. The survey was conducted during June and July 2023, with a sample of 126 respondents, employees of the Croatian national postal operator. The respondents worked in various job positions, including reception, transportation, and delivery of mail, as well as customer service in post offices, across different parts of the Republic of Croatia. The collected data were grouped and presented in Table 1.

The research was conducted through a survey method, using a written questionnaire distributed among employees. This survey had a descriptive-analytical nature, with the questionnaire divided into two main categories of questions. The first category included basic information about the respondents, while the second category examined their opinions on various security factors. The questionnaire comprised ten closed-ended questions, with provided options for responses. The assessment of the current state was carried out through intensity questions, based on a Likert scale with ratings from 1 to 5.

Based on the preliminary research of security factors in various parts of the technological process, it is possible to assess the current state and provide general recommendations for security management using the concept of Tolerable Risk Intensity (TRI). This concept has been developed and applied in other systems but not within the postal system, making this research valuable for the scientific understanding of postal traffic technology and security management (Kemp, 2021).

Regardless of the subject of analysis, risk assessment fundamentally involves identifying, quantifying, and prioritizing risks according to the organization's risk acceptance criteria and objectives (Fereirra, 2019). According to the NIST (*National Institute of Standards and Technology*) method, the risk assessment process includes nine steps:

1. System characterization
2. Threat identification
3. Vulnerability identification
4. Control analysis
5. Likelihood determination of unwanted events
6. Impact analysis
7. Risk determination
8. Control recommendations for risk mitigation
9. Documentation of results (NIST, 2012), (USPS, 2019)

The obtained results should be hierarchically sorted to provide a clear picture of the priorities and needs for applying protective measures to specific system elements (Fereirra, 2019). This methodological framework should be regularly updated and supplemented with new elements introduced into the postal system, such as parcel lockers.

Table 1. Evaluation of the importance of listed security factors in the work process

Security factors	EVALUATION OF THE IMPORTANCE OF LISTED SECURITY FACTORS IN THE WORK PROCESS (%)					
	Excellent (5)	*Very good (4)*	*Good (3)*	*Satisfactory (2)*	*Unsatisfactory (1)*	*Average rate*
At the workplace during the receipt of mail considering working conditions	17	27	41	12	3	3,43
During the X-ray inspection of mail in domestic and international traffic	15	20	38	19	8	3,15
During the transportation of mail from point A to point B	14	31	39	16	0	3,43
During the delivery of mail to the recipient	22	33	32	10	3	3,61
During telephone conversations with customers	27	26	28	17	2	3,59
During the provision of financial services to customers	20	19	40	18	3	3,35
Access to technical protection of persons and property	6	24	36	20	14	2,88
Cooperation with postal security guards and security companies	3	17	36	26	18	2,61
Impact of the existing protection structure on reducing the frequency of threats or attacks on offices/objects	6	19	35	27	13	2,78
Cooperation with the police	5	20	29	21	25	2,59

Most methods for determining and measuring performance indicators of the postal system rely on numerical data, such as accident rates, reports of harmful events, and attacks on vehicles and facilities (USPS, 2019). Surveys and questionnaires are used to assess the level of security in the postal system. Analysis of the results clearly shows where security gaps exist and what needs to be changed to reduce or eliminate risks in the postal system.

The results of the survey conducted among employees of the Croatian national postal operator provide valuable insights into the current state of security within the postal system. By analysing data collected from 126 respondents who perform various jobs within the system, several conclusions and recommendations can be drawn.

The table 1 showing the assessments of security factors reveals variations in the perception of security depending on the workplace and activity. For example, employees expressed the highest satisfaction with security conditions during the receipt of mail (41% rate it as "Good"), while the least satisfaction was with the cooperation with the police (25% rate it as “unsatisfactory”) and postal security guards and security companies (18% rate it as "Unsatisfactory").

The analysis shows that security problems are most pronounced in segments involving physical protection of facilities and cooperation with external security services. For example, only 3% of employees rated cooperation with postal security guards as "Excellent," while 26% rated it as "Satisfactory," indicating a need for improvement in this area.

On the other hand, it is possible to evaluate individual safety factors through average ratings, not just through individual extreme values. However, even in this case, similar indicators of critical safety factors are obtained as with the previous method. In doing so, the overall average rating, which is 3.142, can also be taken into consideration as additional indicator.

Based on the obtained data, the following steps are suggested for improving security procedures:

1. Increasing investment in technical protection by introducing advanced technical solutions, such as modern security cameras, alarm systems, and access controls, can significantly enhance the security of facilities and employees.
2. Improving cooperation with security services through better coordination and communication between the postal system and external security companies can increase the effectiveness of security measures. This includes regular joint exercises, training, and aligning procedures.
3. Employee education through continuous training on security protocols and procedures can reduce the risk of security incidents. Training should cover recognizing suspicious activities, proper handling of security devices, and emergency procedures.

Introducing new security measures always entails certain costs. However, survey results indicate a significant need for improving security conditions, justifying investment in security infrastructure. Strategic investments in security can reduce costs associated with incidents and increase trust among users and employees in the long run.

Using the Likert scale for assessing the current state of security, the obtained data allow the calculation of various security indicators that can be used for continuous monitoring and improvement of security measures. For example, employee ratings can be used to calculate the average level of satisfaction with security conditions and identify areas with the lowest ratings for targeted improvement.

3. CONCLUSION

This research revealed significant variations in the perception of security among employees of the Croatian national postal operator. Key issues in the physical protection of facilities and cooperation with external security services were identified, requiring targeted improvement measures. It is recommended to increase investment in advanced technical solutions, enhance coordination with security companies, and continuously educate employees. Implementing these measures can significantly reduce the risk of security incidents and increase trust among users and employees. The economic justification for investment is supported by long-term cost reductions associated with incidents and damages.

REFERENCES:

Fereirra, J. (2019): Cooperative, *Connected and Automated Mobility (CCAM): Technologies and Applications*. MDPI, https://doi.org/10.3390/electronics8121549

Kemp, A. W. (2021): *Security through cooperation*. Routledge, London. https://doi.org/10.4324/9781003214267

Kowalik, K. (2020): The role of safety in service quality in the opinion of traditional and digital customers of postal service. *Production Engineering Archives*, 26(1) https://sciendo.com/it/article/10.30657/pea.2020.26.01

National Institue of Standards and Technology (2012): *Guide for Conducting Risk Assessments.* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

USPS (2019): *Publication 166 - Guide to Mail Center Security*. https://about.usps.com/publications/pub166/welcome.htm

Xueyan, Y., Changxi, M., Changfeng, Z., Bo, Q., Fuquan, P., Chengming, Z. (2019): Design of hazardous materials transportation safety management system under the vehicle-infrastructure connected environment. *Journal of Intelligent and Connected Vehicles*, 2(1) https://www.emerald.com/insight/content/doi/10.1108/JICV-11-2018-0012/full/html