TRANSCOM 2025: 16th International Scientific Conference on Sustainable, Modern and Safe Transport

Implementation of Information Security Management System in Transport Company

Dominika Findriková[1], Milan Kubina[2]

1 University of Žilina, Žilina, Slovakia
2 University of Žilina, Žilina, Slovakia

INTRODUCTION

Given the advances in the use of new technologies, businesses in various fields, including transport and logistics, need to prepare themselves for the new challenges that come with it. This involves the use of new tools, but also the provision of information and cyber security.

As the use of digital technologies in businesses increases, so does the risk of being the victim of cyber-attacks. The business needs to protect itself physically, but also its information assets. The main stakeholders in this case are business management, IT departments but also employees and customers.

The aim is to introduce the Information Security Management System, to show its possible connection with the strategy and to show the importance of training in this area. The expected impact is to raise awareness in transport companies about information security and to improve the protection of sensitive data.

MATERIALS, METHODS & IMPLEMENTATION

The methods used in this article are qualitative and a qualitative analysis of documents related to Information Security Management System was performed.

- Literature analysis - it was a review of scientific articles whose main topic was Information Security Management System and transport
- Comparative analysis - this was an assessment of potential cyber threats, and a comparison of the information found
- Analysis of case studies - it was about analyzing real examples, there was also an effort to find a real example of a transport company that has implemented Information Security Management System

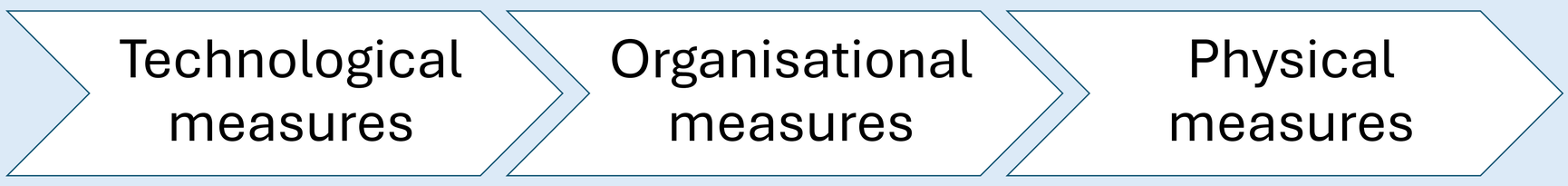
RESULTS

It is safe to say that as long as transport companies implement an Information Security Management System in their processes, they are likely to have their information assets sufficiently well secured.
In the thesis, the main processes that the Information Security Management System includes and thanks to which its implementation can be achieved have been identified. These processes were identified by the authors of the analyzed studies based on a questionnaire among information security professionals. If an enterprise decides to implement an Information Security Management System, it needs to look at three basic elements:

The analyses also showed that there are many processes in transport companies that are vulnerable to possible cyber attacks. These are departments such as the economic department, the marketing department, the logistics department, the HR department, but also processes such as planning. All these processes involve data that is very important and sensitive for businesses. If this information is stolen, destroyed or altered, it could have a very negative impact on the company, its reputation and on its relations with its stakeholders.
Based on the analysis, it is also possible to say that nowadays it is necessary to digitize processes in transport companies and to try to introduce new technologies also to support decision-making.
Similarly, according to analysis from Microsoft's Digital Defense Report 2024, the transportation sector ranks fifth in terms of how much it is affected by cyberattacks. This makes it safe to say that transportation businesses should consider investing in protecting their data and implementing an Information Security Management System.

CONCLUSION & IMPLEMENTATION PATH

Based on the analyses, it can be said that a well-implemented Information Security Management System in transport enterprises is a key step towards securing information assets as well as the overall resilience of the enterprise to cyber threats.
The digitization of processes brings with it advantages such as faster responses to change, flexibility and accuracy, but it also has many disadvantages. These are precisely; it exposes businesses to new threats that come with the use of new technologies. These risks are mainly various cyber threats that can be directed at dispatching, logistics or navigation systems. Their crippling can lead to disruption of business continuity.
It is also important to say that it is not enough to have technical measures in place. To be effective, an Information Security Management System must be aligned with the company's strategy, it must be supported by management and equally accepted by employees.



ACKNOWLEDGEMENTS

Funded by the EU NextGenerationEU through the Recovery and Resilience Plan for Slovakia under the project No.17R05-04-V01-00005.