WORKING PAPER OF THE RESEARCH PROJECT FOR CYBER HYGIENE AND HUMAN FACTORS

Cyber threat factors in port logistics occupational safety

Tuomala, V. *– Project Manager, vesa.tuomala@xamk.fi*

Unit: North European Logistics Institute (NELI)

South-Eastern Finland University of Applied Sciences (Xamk)

(Finland, Kotka)

1. Introduction

The South-Eastern Finland University of Applied Sciences (Xamk) is situated across four cities in two provinces. One of these cities, Kotka, is positioned along the coastline of Finland, near the Finnish-Russian border. Port of HaminaKotka, Finland's largest universal port, serves as a crucial hub for various cargo vessels, facilitating liner services in the Baltic Sea region and Europe, and accommodating international cruise vessels.

The need for this research project emerged in response to the Ukrainian crisis that unfolded in the spring of 2022, specifically Russia's aggressive war against Ukraine. The ongoing conflict in Europe and the subsequent NATO process instigated by Finland have markedly heightened the risk of cyber threats and, information, and hybrid influence. Given the vital importance of ports to Finland, any disruption to their operations or the introduction of chaos through various means could have severe repercussions for Finland's business environment, and security of supply, and pose a threat to occupational safety.

2. Aim and methodology of the project

The project's target groups encompassed operators in port logistics, educational institutions, the city of Kotka, the port of HaminaKotka, companies operating within the area, and relevant authorities. The produced material is specifically tailored for Finnish ports and their collaborators, as well as all small and medium-sized companies in Finland.

The tangible outcomes of the project contribute to enhancing the security and awareness of companies engaged in port logistics, with a particular emphasis on cybersecurity and cyber threats. Post-project, companies will gain a comprehensive understanding of individual employee responsibility and their role in mitigating cyber threats, as well as addressing potential information and hybrid influence, and cyber espionage.

The main theme of the project was safety, which encompasses the overall aspects of the work environment, work community, safety management, and safety competence. Occupational safety entails ensuring that working conditions are in good order, allowing employees to perform their tasks safely. The best way to prevent workplace accidents is through proactive safety measures.

The primary objectives of the project and its steering group were to enhance practical expertise and raise awareness of cyber hygiene among Finnish SMEs closely associated with the port industry. In the realm of cybersecurity, the responsibility for bolstering security does not lie solely within one domain; rather, it necessitates consistent collaboration between management and employees.

The training materials and videos developed in the project were implemented in plain language, deliberately omitting unnecessary "IT jargon" to ensure that the content is easily digestible. All information was presented in a clear and comprehensible manner. The project also aspires to foster similar international collaboration among Baltic and Nordic countries in the future.

The project commenced in early October 2022. Throughout the remainder of the year 2022, efforts were dedicated to scouring scientific publications on cybersecurity from open databases and online services. This involved searching for both domestic and foreign studies and materials. The gathered materials underwent analysis, potential interview questions were formulated, and a comprehensive project description was crafted based on the retrieved material. The project's website, www.xamk.fi/kyberhygienia, was launched on November 9, 2022.

The operational landscape of ports is increasingly digitized, prompting the project to concentrate on enhancing practical-level competence and know-how. Within the project, security is a comprehensive term encompassing both cybersecurity and occupational safety. In our interviews, the target group consisted of businesses operating within the Port of the HaminaKotka.

3. Main outcome of the project

We carried out a total of 17 interviews with employees from various SME companies within the Port of HaminaKotka (of the total 119 corporates), along with a few practice interviews preceding the actual sessions.

Typically, the interviews were conducted through TEAMS connection, with recordings made, registrations noted with IDs, and subsequently transcribed (referential transcription). Following this, the material underwent analysis, and conclusions were drawn from the interviews. The report is readily accessible in the Finnish language on the project's website.

Drawing from the analysis of the interview material, we formulated guidelines for cyber hygiene in the Finnish language. The resulting "Cyber hygiene handbook," crafted within the project, serves as Xamk's versatile information package on cyber threats, information, and hybrid influence for SMEs. It is presented in plain language to ensure comprehensibility for its readers. Additionally, the manual has been translated into English to accommodate the requests of the readers.

As per the project plan, we conducted cyber security and information influencing exercises. The authorities should also be involved in a collaborative exercise within the port sector. We developed easy exercises for companies to implement on their own, drawing on the comprehensive instructions provided by the Finnish National Cyber Security Centre for organizing larger-scale exercises.

4. Implementation of results in practice

The project hosted two seminars with other Xamk’s projects, one in March known as "Cyber Pain Day" and another in September titled "Cyber Autumn Colors" in 2023. In total, there were approximately 250 people present onsite and an additional over 1000 participants online during the seminars. The total cost of these free two seminars was approximately 45,000 Euros. We had an exceptionally high-profile line-up of experts in cyber security and information influence to discuss the current state of security and safety. The feedback from the event was overwhelmingly positive, providing a solid foundation for the possibility of continuing the series of events in the future.

In April 2023, discussions on internationalization and partnership negotiations took place at the Latvian Maritime Academy. Additionally, towards the end of August 2023, the Port Logistics Cyber Hygiene project organized a visit to Estonia, including NATO CCDCOE and TalTech. During this visit, we familiarized ourselves with the operations of the NATO Cooperative Cyber Defence Centre of Excellence, TalTech's Estonian Maritime Academy in Tallinn's Kopli district, and TalTech's Digital Forensics and Cybersecurity Center in Mustamae.

5. Conclusions: Cybersecurity is one element of overall security

In the project, we developed six cybersecurity training videos for micro-studies. These videos are available in Finnish on Xamk's Edufication website under "Welcome to Cybersecurity - Introduction to the Basics". In the first section, cybersecurity RDI expert Tuomas Heikkinen elucidates the meaning of cybersecurity in everyday language through three educational videos. In the second section, Vesa Tuomala guides companies on cybersecurity, cyber hygiene, and human factors, and emphasizes the significance of cybersecurity for critical infrastructure.

The work packages encompassed the following tasks in the funding plan: 1) Mapping and assessing cyber threat factors for occupational safety in port logistics, 2) Analysing, identifying development points, outlining work steps, and generating an informational package for companies, 3) Creating pilot exercises and conducting tests and 4) Organizing a cybersecurity event for port operators.

The objectives of this one-year project were successfully achieved, and the feedback from the Finnish port and maritime sector, as well as SME companies, was positive and encouraging. There is a desire to expand cyber hygiene awareness at the European level. The intention is to establish an international project with potential partners in the port logistics and maritime sector in the Baltic, Balkan, and Ukrainian regions.

The Project Manager, Mr. Vesa Tuomala, also successfully completed a Master's degree in Engineering and Cybersecurity during the project. The materials and findings from his thesis on Human Factor, Cyber Hygiene, Cyber-Physical Systems, and Industrial Control Systems were incorporated into the project. Link to thesis: https://urn.fi/URN:NBN:fi:amk-2023052313040

Literature

1. V. Tuomala, T. Heikkinen. Project Material in the Finnish language internet site of Satamalogistiikan kyberhygienia (Cyber hygiene of port logistics). Xamk. 2023. Available at: www.xamk.fi/kyberhygienia
2. V. Tuomala. Human Factor, Cyber Hygiene, Cyber-Physical Systems, and Industrial Control Systems in the Context of Cybersecurity. Master thesis of Engineering, cybersecurity. Xamk. 2023. Available at: https://urn.fi/URN:NBN:fi:amk-2023052313040