International Journal of Risk and Contingency Management
Volume 14 • Issue 1 • January-December 2026

Supply Chain Risk in the Baltic Sea:
Victim Phenomenology Machine Learning Model

Kenneth David Strang
https://orcid.org/0000-0002-4333-4399
W3-Research, USA & University of the Cumberlands, USA

Bulcsú Székely
https://orcid.org/0000-0003-4593-2277
Lappeenranta – Lahti University of Technology, Finland
Received: December 24th, 2025 | **Accepted:** January 6th, 2026

ABSTRACT

The key objective of this study is to generate a model identifying how decision makers perceive cybercrime risk in logistics supply chain operations taking place in the Baltic Sea Region of the North Atlantic Sea. A mixed-methods approach was applied, using a novel replication-logic case study research design featuring the pragmatist-iterative ideology supplemented with machine learning (ML) to assist with thematic coding. The snowball purposive sampling technique was used to collect online data from confidential informants who worked for large organizations in the Baltic Sea region, after they were cyber-attacked. In the final model, six phenomenological topics across three victim vulnerability keywords were found to be significant. The findings have implications for cybersecurity policy formulation in Europe and globally, where cybercrimes are increasing mostly due to the Russia-Ukraine situation.

KEYWORDS

Logistics Supply Chain, Cybercrime Victim, Digital Transformation, Vulnerability Risk, Machine Learning, System-Thinking, Phenomenology Method

INTRODUCTION

The business problem of our study is that cybercrime continues to disrupt logistic supply chain operations in many industries, despite what we already know about how to prevent it. Ships and other transport vessels are almost entirely reliant on technology for safe operations at sea which makes them at risk of cybercrime either as a direct measure towards the vessel or indirectly through offshore or mainland control operations.

Government, healthcare, and other key disciplinary industries have been adversely impacted by cybercrime. In particular, countries that share their border with Russia are at high risk, namely the Baltic Sea Region. Compounding that risk is the volatile socio-political environment that has developed since several Baltic Sea Region countries joined NATO after Russia refused to stop its invasion of Ukraine. Although strong Western countries have bombed Iran to diffuse social-political and nuclear threats to Israel, thus far, no one other than Ukraine has fought back against Russia. Korstanje (2021) points out that political decision-makers worldwide have become complacent to

DOI: 10.4018/IJRCM.398934

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

thana capitalism meaning that monetary greed has overpowered morality to the extent cybercriminals may attack vessels in the Baltic Sea simply to terrorize rig workers.

Geo-political tensions were very high worldwide in 2025. There was clear evidence of healthcare, government, and other industry-specific cybercrime in the Baltic Sea Region. Norway, Sweden, and Finland are prominent countries in the Baltic Sea Region that have been impacted by cybercrime risk. For example, the Information Technology Director at a large Finland-based healthcare supply chain provider (Solteq Public Limited Company) warned that the recent data breaches were a wake-up call for Chief Executive Officers (Kulmala, 2025). In the Vincit cybersecurity supply chain cyber attack, cyber criminals stole healthcare data of 70,000 clients of the Valio Corporation – this was one of several companies of Vincit that were hacked (we are unaware of the full extent of that data breach).

Employees of companies in the Baltic Sea Region may be more likely to be cybercrime victims as compared to unemployed individuals. Employees tend to have economic assets and corresponding vulnerability to cybercriminals. Cyber criminals often seek economic payouts or political gains from vulnerable groups of people, such as company employees or clients, rather than targeting individuals (Strang, 2025; Tuteja, 2025). Thus, organizational managers and executives need to take action to protect their employees and customers from cybercrime. In fact, the Finnish National Cybersecurity Center had earlier sent a public note to warn organizational decision makers and employees about an emerging massive data breach wave in October 2023 (Finnish Transport and Communications Agency, Traficom 2023).

Cybersecurity logistics supply networks do not seem to function seamlessly anymore. According to the literature, this is due to the massive scale of system coordination problems (Alqudhaibi et al. 2025; Meijas et al. 2025; Kour, et al. 2025; Piper 2025a,b; West 2025; Generao and Leonhirth 2025; Baron et al. 2025; Lyon, K. and Serban 2025; Strang and Vajjhala 2024; Fatima et al. 2024; Brown et al. 2024). Common symptoms of this type of cooperation fatigue include increasing cyber-criminal capabilities, technological complexity, and a lack of victim training and awareness. Therefore, comparing cases of organizational systems experiencing cyber violence is imperative to minimize the potential financial losses looming on the horizon.

A corresponding issue is that the existing literature tends to focus on the cyber criminal, the overall historical trends or the philosophical aspects of cybercrime (Korstanje, 2021). There is very little mention of cybercrime in the Baltic Sea Region and not enough empirical research from the victim perspectives of cyber criminal behavior. We need a deeper analysis of the victim's perception of cybercrime reasons and impacts.

Subsequently, the research question (RQ) was to identify what logics supply chain decision-makers in Baltic Sea Region supply chain business think about cybercrimes in terms of the psychological reasons and impacts. The authors wanted to get inside the heads of actual supply chain business victims to understand the reasons for and impacts of cybercrime. The goal was to develop a phenomenology of cybercrime victim vulnerability thematic model. Instead of employing the traditional phenomenology interview transcript thematic coding technique, the authors relied entirely on machine learning (ML) techniques to analyse the data collected from confidential informants of cybercrime.

LITERATURE

This section is divided into three parts to group together the similar literature into quantitative, then qualitative, and finally mixed methods type of papers. The scope of our literature review was all peer-reviewed journals, conferences, edited books, edited book chapters, and good-quality peer-reviewed papers. We primarily targeted open-access papers since these are leading the way to high-powered scientific knowledge sharing.

14 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/supply-chain-risk-in-the-baltic-sea/398934

Related Content

Cloud Risk Resilience: Investigation of Audit Practices and Technology Advances - A Technical Report
Akhilesh Mahesh, Niranjali Suresh, Manish Guptaand Raj Sharman (2019). *International Journal of Risk and Contingency Management (pp. 66-92).*
www.irma-international.org/article/cloud-risk-resilience/227022

A Critical Review of Information Technology Innovations
Ruben Xing, John Wangand Qiyang Chen (2013). *International Journal of Risk and Contingency Management (pp. 63-78).*
www.irma-international.org/article/a-critical-review-of-information-technology-innovations/80021

The VESP Model: A Conceptual Model of Supply Chain Vulnerability
Arij Lahmar, Habib Chabchoub, François Galassoand Jacques Lamothe (2018). *International Journal of Risk and Contingency Management (pp. 42-66).*
www.irma-international.org/article/the-vesp-model/201074

Libraries to the Rescue
Michael R. Mabe (2016). *International Journal of Risk and Contingency Management (pp. 62-81).*
www.irma-international.org/article/libraries-to-the-rescue/148214

How Lean Six Sigma Risk Management Was Used at a Clean Energy Plant
Kenneth David Strang (2022). *Global Risk and Contingency Management Research in Times of Crisis (pp. 76-98).*
www.irma-international.org/chapter/how-lean-six-sigma-risk-management-was-used-at-a-clean-energy-plant/306567