UNIVERSITI TEKNOLOGI MARA

5th I-CReST 2025

INTERNATIONAL CONFERENCE ON RESEARCH AND PRACTICES IN SCIENCE, TECHNOLOGY AND SOCIAL SCIENCES

SYNERGY FOR FUTURE SUSTAINABILITY:
BRIDGING SCIENCE, TECHNOLOGY AND HUMANITIES

Abstract Book

UNIVERSITI TEKNOLOGI MARA
CAWANGAN SELANGOR, KAMPUS DENGKIL
MALAYSIA

13th SEPTEMBER 2025

ORGANISED BY: Centre of Foundation Studies

STRATEGIC PARTNER: UiTM Global

IN COLLABORATION WITH: UTM

I-CReST 2025:076-042 – Sailing into Cyber Awareness: Determinants of Security Behaviour Among Seafarers

Hasivini Manaoogaranand and *Noor Fadhiha Mokhtar

Faculty of Business, Economics and Social Development, Universiti Malaysia Terengganu, 21030 Kuala Nerus, Terengganu, Malaysia.

*E-mail: noorfadhiha@umt.edu.my

ABSTRACT

The maritime industry is increasingly vulnerable to cyber threats, as demonstrated by the 2017 Maersk cyberattack, which exposed the fragility of global shipping operations. With the growing integration of digital technologies into shipboard systems, ensuring robust cybersecurity awareness among maritime personnel is more crucial than ever. However, empirical research on the human and behavioural factors influencing cybersecurity awareness in maritime contexts remains limited. This study investigates the influence of self-efficacy, perceived benefits, cues to action, and perceived susceptibility on the cybersecurity awareness of seafarers. Grounded in the Health Belief Model—a well-established framework from preventive healthcare adapted in this study to understand users' computer security behaviour. This study employs a quantitative approach to examine hypothesised relationships among these variables. Data were collected through structured questionnaires administered to seafarers who regularly operate computer systems, and statistical analysis was conducted to evaluate the strength and significance of the relationships. Findings reveal that perceived benefits and cues to action significantly contribute to improving cybersecurity awareness. In contrast, perceived susceptibility emerged as a weaker predictor. This is likely due to seafarers' limited experience with actual cyber incidents and the common belief that such threats mainly affect shore-based systems. Incident-based training and realistic simulations are recommended to clearly demonstrate the operational impact of cyberattacks on shipboard environments. This study contributes to the growing body of literature on maritime cybersecurity by addressing a gap concerning human factors in information security behaviour. It offers practical implications for maritime organisations, shipping companies, and policymakers seeking to strengthen cyber resilience. Promoting continuous training and awareness initiatives can help foster a proactive cybersecurity culture among seafarers and mitigate risks associated with human error in digital maritime operations.

Keywords: Maritime Cybersecurity; Cybersecurity Awareness; Health Belief Model; Seafarers and Maritime Digitalization