Taylor & Francis
Taylor & Francis Group

Journal of International Maritime Safety, Environmental Affairs, and Shipping

ISSN: 2572-5084 (Online) Journal homepage: www.tandfonline.com/journals/tsea20

Building cyber-resilience in maritime transport: A stakeholders' perspective on mitigation measures

Changki Park, Christos Kontovas, Zaili Yang & Chia-Hsun Chang

To cite this article: Changki Park, Christos Kontovas, Zaili Yang & Chia-Hsun Chang (2025) Building cyber-resilience in maritime transport: A stakeholders' perspective on mitigation measures, Journal of International Maritime Safety, Environmental Affairs, and Shipping, 9:3-4, 2594832, DOI: 10.1080/25725084.2025.2594832

To link to this article: https://doi.org/10.1080/25725084.2025.2594832

Published online: 04 Dec 2025.

JOURNAL OF INTERNATIONAL MARITIME SAFETY, ENVIRONMENTAL AFFAIRS, AND SHIPPING
2025, VOL. 9, NOS. 3–4, 2594832
https://doi.org/10.1080/25725084.2025.2594832

Building cyber-resilience in maritime transport: A stakeholders' perspective on mitigation measures

Changki Park[a,b], Christos Kontovas[a], Zaili Yang[a] and Chia-Hsun Chang[a]

[a]Liverpool Logistics, Offshore and Marine Research Institute (LOOM) and School of Engineering, Liverpool John Moores University, Liverpool, UK; [b]Department of Global Commerce, College of Economics and International Commerce, Soongsil University, Seoul, South Korea

ABSTRACT

Cybersecurity risks are becoming a major concern in the maritime industry due to the increasing reliance on information technology and operational technology systems. This paper aims to develop a new methodology to evaluate the effectiveness of risk control measures (RCMs). Six criteria influencing the choice of cybersecurity RCMs are identified through literature review. Expert opinions are used to assess major cybersecurity RCMs using the fuzzy TOPSIS (Technique for Order Preference by Similarity to Ideal Solution) method. The methodology prioritises the most viable RCMs using primary data collected from 100 experts. The findings indicate that the most effective cybersecurity control measures based on stakeholders' opinions are "Effective Antivirus software management," "Management of network devices," and "Developing a cybersecurity strategy." This paper contributes to maritime cybersecurity policy guidance by providing experimental evidence and offers a new decision tool to aid stakeholders in selecting the most suitable measures to address the relevant risks.

ARTICLE HISTORY
Received 8 July 2024
Accepted 14 November 2025

KEYWORDS
Maritime cybersecurity; fuzzy TOPSIS; multicriteria decision making analysis; cybersecurity mitigation strategy

Introduction

The maritime industry plays a central role in economic sustainability. With the rise of Shipping 4.0 (as the maritime extension of Industry 4.0), more and more software and hardware systems are being used in the industry both on vessels and shore-based infrastructure. Onboard vessels, navigational and power-related systems increasingly depend on software and hardware, making technology essential for safe and secure operations. At the same time, digital connectivity and online communication access are crucial to seafarers as they are linked to their sense of well-being, crew cohesion, and social isolation (Jensen, 2021).

The shipping industry has long dealt with safety considerations, and for the past couple of decades, with security-related issues such as the prevention of piracy and armed robbery against ships, counter-terrorism, stowaways, drug smuggling, and other concerns. However, the above-mentioned increasing reliance on information communication technology in international trade has raised concerns related to cybersecurity (Chan & Choi, 2023; Kanwal et al., 2022; Lin et al., 2022; Mohsendokht et al., 2024). These concerns are not only relevant to the shipping industry but will affect all transport modes and will be aggravated by the increased use of autonomous means (Chang et al., 2021). Ports are also facing similar issues; the main driver of changes in the sector is considered to be their digital transformation into "smart ports" and, therefore, cybersecurity is now considered one of the main threats to the port industry (De la Peña Zarzuelo, 2021; Martín-Duque et al., 2023).

In addition to the advancement of autonomous shipping as mentioned above, there is noteworthy evidence indicating that the COVID-19 pandemic has triggered a substantial surge in the adoption of digital tools within the shipping industry (Bolbot et al., 2022). This surge is closely tied to the growing imperative for decarbonisation and involves various initiatives, including the adoption of cleaner fuels, energy-efficient technologies, and alternative propulsion systems in the shipping sector. These unquestionably entail

CONTACT Chia-Hsun Chang c.chang@ljmu.ac.uk Liverpool Logistics, Offshore and Marine Research Institute (LOOM) and School of Engineering, Liverpool John Moores University, 3 Byrom Street, Liverpool, L3 3AF, UK

Present affiliation of Changki Park: Department of Global Commerce, College of Economics and International Commerce, Soongsil University.

ramifications for cybersecurity. Many of these decarbonisation measures necessitate the incorporation of digital technologies, sectors, and control systems to optimise vessel operations, reduce energy consumption and thus improve the environmental footprint. An illustrative example can be found in the deployment of sensors for monitoring fuel consumption and the implementation of remote monitoring and control systems for energy-efficient technologies and pumps. The maritime industry's increased focus on decarbonisation has a parallel impact on seaports. These ports, in their pursuit of reduced emissions, have become more exposed to potential cyberattacks as well; see Alzahrani et al. (2021).

Failure to address these cyber-risks could lead to severe consequences such as human fatalities, economic damages, loss of reputation, environmental impacts, and more. This has been evident from incidents such as the cyberattack on Maersk, which resulted in a loss of $200–300 million in 2017, as well as the cyberattacks suffered by the COSCO terminal at Port of Long Beach in 2018, the International Maritime Organisation (IMO) and CMA CGM in 2020, with network breakdowns lasting several days. Chang et al. (2019) presented a table of maritime cyberattack incidents from 2011 to 2018. A list of maritime cyberattack incidents from 2019 to 2023 is presented in Appendix A. In addition, Meland et al. (2021) showed that the number of maritime cyberattack incidents grew in a non-linear trend from 2015. With such increasing concerns on maritime cybersecurity, the shipping industry is urgently seeking measures to address cyber risk from both administrative and regulatory (e.g., the IMO) and operational (e.g., shipowners or operators) perspectives. For a comprehensive discussion on maritime cyberattacks, including their frequency and impact, interested readers are referred to Mohsendokht et al. (2024).

In July 2017, the IMO adopted its first-ever guidelines on "Maritime Cyber Risk Management" to address the relevant concerns; see IMO (2017). According to the guidelines, maritime cyber risk refers to *"a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised"* (IMO, 2017). In addition, the IMO adopted a resolution that encourages maritime administrations to *"ensure that cyber risks are appropriately addressed in existing safety management systems"* - this means as part of their compliance with the International Safety Management (ISM) Code.

However, several studies contend that current cybersecurity guidelines and approaches in the maritime sector are not enough to keep important data and assets safe from cyber threats. Hopcraft and Martin (2018) suggested that the IMO needs to produce a strong and resilient standalone maritime cybersecurity regulation, based on a framework similar to other IMO Codes such as the Polar Code. Karahalios (2020) investigated security concerns in three different companies within the context of a piracy attack. He identified that pirates could take advantage of communication and navigation security weaknesses, and thus suggested the applications of strong physical security and primarily control internet access. However, he also argued that the training, awareness, and company policies were still insufficient. Drazovich et al. (2021) insisted that comprehensive guidelines are needed, as current maritime cybersecurity guidelines are insufficiently grounded, and do not provide a set of holistic recommendations to the key stakeholders. Karim (2022) called for a more collaborative approach between different actors (e.g., UN agencies) and highlighted the inadequacy of the maritime cybersecurity IMO legal instruments, for example, the fact that they are not legally binding. There is also a clear need to rethink the approach to these risks. Cybersecurity cannot easily be approached using traditional risk assessment methods; one reason for that is the absence of historical information on cyber-attacks (see Sheehan et al., 2019). At the same time, there have been some attempts to link safety and security methods; see Fan and Yang (2022) for more.

Although showing some attractiveness, the current IMO Guidelines on maritime cyber risk only provide high-level recommendations and are, therefore, not specific enough for the frontline operators to use and adopt them immediately. At the same time, the IMO suggested "risk management" as an approach to addressing cyber-risks. They refer to several guidelines and industry best practices, amongst others, the BIMCO-led Guidelines (BIMCO, 2020) which proposes that cyber risk management should include the implementation of *"technical and procedural measures to protect against a cyber incident, timely detection of incidents and ensure continuity of operations."* In fact, and in line with common practices (see, for example, the ISO Standard 31,000:2018 "Risk management – Guidelines"), "risk treatment" follows the "risk assessment" process, which consists of (a) the identification of risk, (b) risk analysis and (c) risk evaluation; the latter is related to comparing the results with acceptable risk levels in order to determine whether risk treatment measures are needed to be implemented (ISO, 2018). Following a comprehensive risk assessment, options

for treating the risk should be considered; these might include options to avoid the risk, remove the risk source, and reduce the likelihood or the impacts of adverse events. BIMCO (2020) provides a detailed description of developing protection measures discussing various technical measures (e.g., as the limiting and controlling of network ports, protocols and services, using physical security measures such as restricting the use of USB ports, patch management, etc.) and procedural measures (e.g., training and awareness, software maintenance, anti-virus management). Detection measures such as scanning software for malware detection are also discussed.

In light of the above, our research aims to analyse the effectiveness and efficiency of a set of cybersecurity mitigation measures currently being promoted in various guidelines or used in practice. Selecting appropriate risk control measures (RCMs) is not an easy task as it involves balancing the potential benefits derived from their implementation against the costs, effort, or disadvantages of their implementation. To identify the most cost-effective solutions, this paper uses a Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) methods because of its wide use, easiness and advantages compared to the other Multiple Criteria Decision Making (MCDM) techniques. Some advantages of TOPSIS over other MCDM methods include its user-friendliness, effectiveness in handling complex decisions, and its ability to provide clear and easily understandable rankings for decision-makers (Belabyad et al., 2025).

We evaluate and rank the most used RCMs against six criteria which are identified through a thorough literature review. In the process, the six criteria are validated and weighed by domain experts who have experiences in the maritime sector industrial or academic. Furthermore, the advantages and disadvantages of each alternative RCM against the criteria are presented for useful insights into policy making. In line with the IMO Guidelines (IMO, 2017), which recognise that organisations are different, in our study the RCMs are expressed in broad terms for a more widespread application and to be compatible with the Guidelines.

It is anticipated that these measures will help prevent potential cybersecurity incidents and mitigate their adverse impacts. Having a set of preparedness and prevention measures to decrease security threats can enhance the resilience capability of companies. This is supported by empirical studies that have demonstrated the importance of security management practices in bolstering the resilience of maritime companies (Yang & Hsu, 2018).

In line with Logan et al. (2022), our stance is that adopting risk-based approaches provides a comprehensive path to building resilience. Consequently, the implementation of various risk control measures can augment the cyber-resilience of companies. This enhancement aids both ship-based and shore-based systems (including ports) in their capacity to "sustain or attain intended functionality" in the aftermath of a cyber incident. Our array of control measures encompasses both preventive controls, which are designed to avert or withstand cyber events, and responsive controls, which are instrumental in mitigating potential consequences.

This work therefore makes original and novel contributions, including a) the development of a new methodology to enable the effective evaluation of cybersecurity RCMs; b) the identification of essential criteria for supporting the evaluation; c) the collection of empirical data to rank the currently established RCMs; and d) the provision of risk-informed policymaking for rational maritime cybersecurity assurance. Ultimately, the research lays the groundwork for risk-informed policymaking in maritime cybersecurity. Its methodology can also be applied to similar areas, especially cybersecurity in related sectors like transportation and logistics.

Literature review, research gap, and problem setting

Relevant literature and research gap

Amid the growing apprehension surrounding maritime cybersecurity, the IMO, the BIMCO, DNV, the American Bureau of Shipping (ABS), the United States Coast Guard (USCG) and several other classification and government organisations have published maritime cybersecurity guidelines; see Progoulakis et al. (2021) for a detailed survey of the relevant literature. It is worth noting that many of these documents fall into the so-called "grey literature" – that is outside the traditional academic publishing channels.

In February 2016, the BIMCO, the world's largest international shipping association representing 60% of the world's cargo fleet measured by tonnage, led an industry initiative publishing the first-ever "Guidelines

on Cyber Security onboard Ships" (BIMCO, 2016) and it was published Vol. 4 in 2020. The IMO released in June 2022 the "Guidelines on Maritime Cyber Risk Management" (MSC-FAL.1/Circ.3/Rev.2), which supersedes the interim guidelines contained in MSC.1/Circ.1526 published in June 2016.

However, in the academic area, compared to other topics in the maritime sector, the research related to maritime cybersecurity is relatively limited. Park et al. (2023) conducted a bibliometric analysis using the Scopus database, revealing 159 documents after excluding the ones that were not relevant to the maritime/shipping industry, in which only around half of them (i.e., 75 documents) are journal papers. This highlights the fact that the literature is still scant, but the area is receiving increasing attention. Another interesting finding is that much of the literature is related to risk management but the papers that evaluate the importance of the RCMs are relatively few. At the same time, very few papers (indexed by Scopus) use an MDCM technique to address maritime cybersecurity; we could only identify three empirical studies. Karahalios (2020) addressed maritime cybersecurity using fuzzy Analytic Hierarchy Process (AHP) to evaluate the severity of each security constraint; Knight and Sadok (2021) used normal statistic descriptive analysis and Yoo and Park (2021) also utilised the AHP method.

The interested readers are referred to Progoulakis et al. (2021) and Bolbot et al. (2022) for two very comprehensive surveys of the maritime cybersecurity domain; the latter summarises also the relevant literature survey papers. Progoulakis et al. (2021) present the relevant standards, guidelines and a survey of relevant academic papers, with risk analysis and assessment methods being the main focus of their survey. Bolbot et al. (2022) present a bibliometric analysis and a very comprehensive review of the area, along with the research directions. In line with our findings and the work of Progoulakis et al. (2021), their analysis demonstrated that the main research focus in maritime cybersecurity is indeed on *"the development or application of cybersecurity risk assessment techniques and the design of monitoring and intrusion detection tools for cyberattacks in maritime systems."*

Based on the above there is a gap in the existing literature on maritime cybersecurity. In addition, we envisage cybersecurity to attract more and more research as the body of literature on autonomous shipping is expanding as well. As the level of autonomy will be increasing so will the dependence of ships on IT and Operational Technology (OT) systems, increasing the overall cybersecurity risks. Chang et al. (2021) have identified "cyber-attacks" as the second most important hazard for autonomous vessels. The result is also supported by Cao et al. (2023) who conducted a bibliometric analysis of marine accidents with 491 literatures in the Web of Science database.

Problem setting

To avoid the consequences of cyber-attacks, the relevant risks need to be addressed. Threats and vulnerabilities should be identified, and protection and detection measures should be developed to reduce the risks; this can be done by reducing the likelihood of the vulnerabilities being exploded and/or reducing the impact.

In this study, we aim to provide high-level recommendations and therefore the RCMs are expressed in a broad term. To achieve this, the most used RCMs (or "alternatives" in the MCDM terminology) are identified based on literature review (see Measures for assessing mitigation measures for more) and discussion with experts. MCDM methods have been employed to select a favoured option, categorizing alternatives into groups, and/or establishing a subjective preference ranking for the alternatives; see Behzadian et al. (2012) for a survey on the classical and fuzzy TOPSIS state-of-the-art, respectively, their applications, advantages, and main challenges.

In this study, a fuzzy TOPSIS approach is applied; a comparison of our results with other methods is presented to validate the selected methodology. A comparison of fuzzy approaches is offered by Ceballos et al. (2017); there is much evidence that a number of approaches lead to similar, if not the same, ranks. This is an important result as our methodology utilises the fuzzy TOPSIS methodology to rank a number of alternatives in an attempt to provide useful managerial insights. In this sense, the robustness of the results can be ensured (as similar methods would arrive at the same results) and, therefore, so do our recommendations.

To summarise, through a literature review (see Measures for assessing mitigation measures for more) and discussions with experts, seven RCMs to reduce maritime cybersecurity risks and six criteria for assessing

them have been identified and discussed in more detail in the following sections. Figure 1 illustrates the hierarchy structure and presents the relationship between the above-identified criteria and the measures or strategies to be assessed.

Measures for assessing mitigation measures

Education and training

Providing new employee orientation and ensuring all personnel are regularly trained is crucial. Educating and training sea crew and staff is argued to be an effective approach to strengthening maritime cybersecurity (Corallo et al., 2022; Jones et al., 2016). These papers suggest that sea crews should be educated to deal with cyber incidents manually to protect the onboard systems and reduce damage to the equipment. Zhang et al. (2020) stated that insufficient training would be a significant reason for the operation failure of vessels and addressed that stakeholders should be mandated to participate in a training program. Nevertheless, there is limited discussion on how companies can educate seafarers to deal with existing threats (Canepa et al., 2021; Karahalios, 2020). Therefore, the BIMCO (2018) stated that the maritime industry lacks a cyber awareness culture, which could result in more sources of vulnerabilities and thus cause more cyberattack incidents. The IMO decided to enhance cybersecurity awareness; shipping companies are required to develop cybersecurity management systems, from the 1 January 2020; see IMO document MSC. 428 (98). A number of class societies offer relevant awareness programmes; for example, the Korean Register (KR) provides a cybersecurity education programme to train crew on how to increase their cybersecurity awareness, including the identification of cybersecurity threats. This is becoming increasingly necessary, especially given the rise of misleading content. Discussions around deepfake technology highlight this issue (Kumar et al., 2024), and it's crucial to protect seafarers from such threats.

Effective antivirus software management

The BIMCO (2018) found that the number of maritime cyber incidents has reached critical situations because of the failure of software maintenance and patching. They emphasised the necessity of installing an antivirus program on all work-related computers onboard vessels to reduce the possibility of systems being cyber-attacked. Moreover, they found that uninstalling anti-virus programs might result in data loss, unauthorised access to data or information, and network connection losses (Boyes & Isbell, 2017; Guanah, 2021)

Hardware and software maintenance

Updating onboard security and safety systems should be an essential priority. That is the case for important OT systems such as Supervisory Control and Data Acquisition Systems, Global Positioning Systems (GPS), and Distributed Control Systems (DCS). These kinds of systems have a long lifecycle and

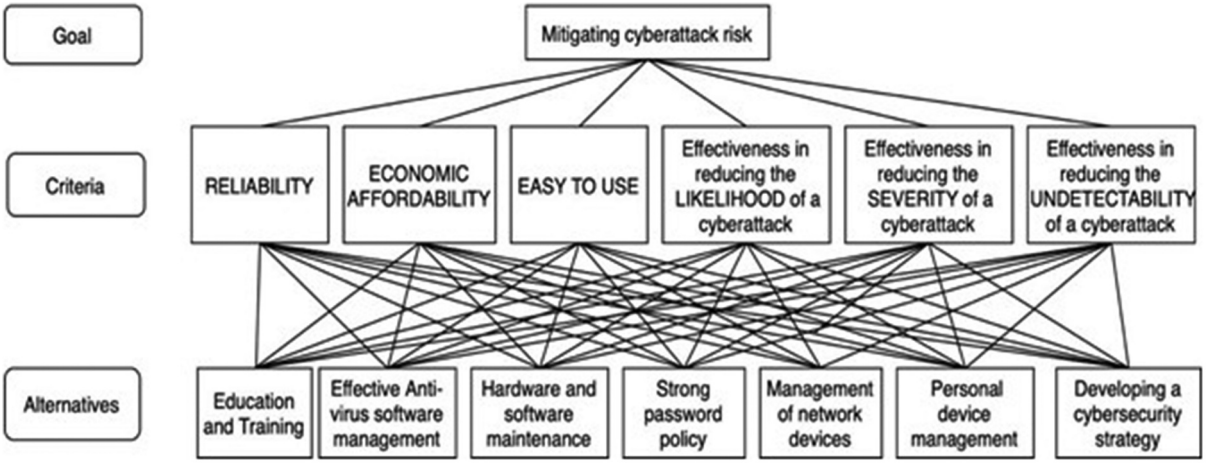

Figure 1. Hierarchy of maritime cybersecurity RCM evaluation.

should be maintained and patched regularly; this is critical in mitigating cyber risk. However, sometimes, updates would not be received for any software or hardware that stops being supported by its software developer or producer (Guanah, 2021). To keep software updated to the latest version, a schedule of maintenance cycles should be a key priority of software providers as well (Fischer-Hübner et al., 2021; Lagouvardou, 2018). It is necessary to always update software systems to the latest versions to mitigate cyber risks (Bolbot et al., 2020; Fitton et al., 2015). This is due to the simultaneous development of advanced technology, which leads to the creation of numerous viruses and malicious programs. Consequently, the maritime industry must update or even upgrade its IT systems not only to combat the threat of cyberattacks but also to maintain competitiveness (Svilicic et al., 2020). Additionally, using the latest software can be beneficial, as software designers are creating increasingly durable applications by incorporating durability concepts like automated code reviews (Kumar et al., 2023).

Strong password policy

Mandating the use of complicated passwords and requiring users to change them regularly are widely recognised as a low-cost and easily implemented measure against cyber threats (National Cyber Security Centre, 2019). Poor password practice could cause unauthorised access and data breaches (IMO, 2017). The lack of password management, especially in the shipping industry, is exasperated by the fact that many vessel systems are used by multiple crew members who all share passwords (Alcaide & Llave, 2020). Therefore, a strong password policy is recommended to deal with the risk of unauthorised access (Bolbot et al., 2020; Koola, 2018). Ensuring a strong password policy could include a mandate to update passwords regularly and to use multi-factor authentication, where possible (BIMCO, 2018).

Personal device management

Recently, the use of Bring Your Own Device (BYOD) – refers to being allowed to use one's personally owned device, rather than a company provided device – such smartphones have been extended in the information and communication environment. Cyberattacks are also rapidly changing from traditional information and communication systems to infrastructure control systems, requiring structural changes in vulnerability analysis and evaluation methods (Dellios & Papanikas, 2014). Personal devices such as laptops, smartphones, and USB drives could be used to install malicious programmes into operational and information systems. Hardware vulnerabilities largely pertain to the reliability of the system and the data on it. For instance, ECDIS can be updated via USB drives or the Internet; during this process, unauthorised USB drives may cause data loss or load malicious programs to OT systems (Pseftelis & Chondrokoukis, 2021). Therefore, effective personal device management can ensure that the crew's personal devices (e.g., smartphones and laptops) cannot access sensitive systems such as the ship's navigation systems and other network critical areas.

Management of network devices

Most devices/systems do not operate in isolation; they communicate with each other – that is they are part of a network – and can also be accessed from the "outside" world. There are several cyberattack threats, such as network protocol attacks, network monitoring and sniffing. Network device configurations such as the use of proxy servers, encryption, firewalls, and Virtual Private Networks (VPN) are countermeasures for network protocol attacks and could be used to determine which systems should be attached to controlled or uncontrolled networks to prevent any security risks through connected devices (Boyes & Isbell, 2017; Jang-Jaccard & Nepal, 2014). Network systems that should be placed on controlled networks include networks that are used to provide suppliers with remote access to OT software and networks that are necessary for the operation of a vessel. Misconfigured firewalls and proxy servers can cause errors in network systems onboard vessels and ashore (BIMCO, 2020).

Developing a cybersecurity strategy

Several guidelines recommend setting up cybersecurity strategies to protect assets from cyberattacks and to guide the actions should cybersecurity incidents happen. The IMO (2017) has issued a document entitled

"Guidelines on maritime cyber risk management" suggesting five functional steps that support effective cyber risk management: "Identify, Protect, Detect, Respond, Recover." BIMCO (2016) also suggested a similar cyber risk management approach with the following steps: *"Identify threats, Identify vulnerabilities, Assess risk exposure, Develop protections detection measures, Establish contingency plans, Respond to and recover from cybersecurity incidents."*

Assessment criteria

Having identified a number of RCMs to mitigate the cybersecurity risks, the next step is to identify a set of criteria that can be used to assess them. This is a common approach in dealing with MCDM problems; different alternatives (in our case the RCMs presented above in Relevant literature and research gap) are assessed based on a set of criteria to establish a comparison among the alternatives. The selected criteria as well as the relevant literature suggesting or/and supporting the use of the specific criteria are presented below.

Reliability

Reliability has been identified as an important factor in determining a cyber risk strategy (Li & Kang, 2015). In the context of this work, it refers to the capability of the said measures to perform as designed, also under particular conditions, and to their durability in case of failure.

Economic affordability

Although the number of cybersecurity incidents has been rising, all relevant players, e.g., shipping companies and port authorities have financial constraints to address cybersecurity risks. According to Hayes (2016) and Lee and Wogan (2018), the majority of companies spend 1~2% of their overall budget on cybersecurity management. Therefore, it is of extreme importance for companies to utilise their limited budget cost-effectively. Affordable measures are therefore the ones that do not cost much to purchase and operate over their lifetime.

Ease of use

Cybersecurity RCMs that are simple (for example, in their design, use, and implementation) are the ones that are preferred by the industry (BIMCO, 2020). Sea crew who only have a basic level of knowledge of cybersecurity might have difficulties understanding the concepts and mechanisms of complicated cybersecurity and the relevant measures. Therefore, it is imperative to apply cybersecurity measures and strategies that are easy to use (Pseftelis & Chondrokoukis, 2021). This criterion refers to how straightforward and simple it is to use/implement the strategy (Poghosyan et al., 2020).

Effectiveness in reducing the risk of cyberattacks

It is essential that the proposed measures can effectively reduce cybersecurity risks. The alternatives should therefore be assessed based on their effectiveness in terms of overall risk reduction. Failure Mode and Effects Analysis (FMEA), as a common method for risk assessment, presents a systematic approach based on three attributes: (a) the likelihood of failure, (b) the consequence of severity, and (c) the probability of the failure being undetected. FMEA has been widely applied in the maritime sector (Chang et al., 2021; Yang & Wang, 2015; Yang et al., 2008).

In this paper, following the concept of FMEA, we assess the effectiveness of the defined alternatives through the three risk parameters. The likelihood part refers to how important the effectiveness in reducing the likelihood of being cyberattacked is in the selection of the best alternative i.e., mitigation measure to be introduced. The second attribute is the effectiveness in reducing the severity of being cyberattacked; this refers to the effects/consequences following an attack. These can be financial loss, loss of reputation, loss of life, environmental damages, etc. Finally, we look at the third aspect – this is related to detectability. There are, for example, cases where cyberattacks can be detected before adverse consequences occur. Many threats, though, are not easily detected or, in practice, are undetectable. We therefore assess the different measures/strategies, assessing their effectiveness in reducing the

undetectability of cyberattacks, which is tantamount to assessing their effectiveness in reducing the probability/likelihood that the harm will occur.

Detectability is indeed very important; even though many trustable architectures have been proposed (see Wang et al., 2022) many attacks, at least at their initial stages, are undetected. Some cyberattacks on the IT/OT systems may involve a continuous alteration of nautical data across multiple messages to deceive various sensors simultaneously, while also evading potential integrity checks (Hemminghaus et al., 2021). Malicious programmes can stay undetected within the system specifications. According to Wimpenny et al. (2021), a security vulnerability has been detected in the authentication scheme security weakness was identified with the authentication scheme. In an extreme, but real, example of an undetected case, the cyberattack on the Danish Maritime Authority (DMA), which started in 2012, was only discovered in 2014. It has been found that a PDF (Portable Document Format) document was infected with a virus, which propagated from DMA to other government organisations (Chang et al., 2019). In addition, some cybersecurity threats, such as phishing or man-in-the-middle attack, can indeed steal important data or information without being even noticed (Ashraf et al., 2022).

Methodology

As outlined above, the paper addresses the issue of identifying effective cybersecurity RCMs. We assess the various measures and produce a rank, which can help identify the "best" measures. This is important so that the industry directs its efforts towards the measures that stakeholders believe are the most important ones. The proposed fuzzy TOPSIS approach (following the classical approach as per Hwang and Yoon (1981)) is briefly described below to keep the work self-contained.

Classical TOPSIS and Fuzzy TOPSIS

TOPSIS is a widely used method for ranking alternatives based on the concept that *"the best alternative should have the shortest distance from the positive ideal solution (PIS) and the longest geometric distance from the negative ideal solution (NIS)"* (Hwang & Yoon, 1981; Hwang et al., 1993). It has a long history and is known for its simplicity and practicality in various fields (Belabyad et al., 2025; Chukwuka et al., 2024; Tyagi et al., 2018; Yeo et al., 2023; Zhang & Lam, 2019). It is chosen for this research due to difficulties in obtaining reliable data. For a literature review of TOPSIS applications about its applications, advantages, and challenges, see Behzadian et al. (2012).

In the classical TOPSIS approach, the performance ratings and the weights for the criteria are provided as crisp values. This paper utilises the fuzzy TOPSIS method, initially introduced by Chen in 2020, which acknowledges that human judgment is often too complex to be captured by precise numbers. In fact, the use of fuzzy sets allows for the incorporation of unquantifiable, incomplete, non-obtainable information, and partially ignorant facts into the decision model and is preferred compared to the classical TOPSIS (Dağdeviren et al., 2009). Therefore, a linguistic assessment for the ratings and the weights of the criteria is used.

The extension of the TOPSIS to a fuzzy environment is straightforward; the approach is very similar to that of the classical TOPSIS. The main difference is that fuzzy numbers are used instead of crisp numbers and fuzzy arithmetic is utilised; please see Appendix B on the theory basics and arithmetic. The methodology, which is illustrated in Figure 2, consists of the following steps.

Step 1. Problem definition and data collection

The problem is defined, i.e., by identifying the alternatives and the criteria that will be used in assessing them (see Figure 1). This can be done through a literature review; see Section 2.1 and Section 2.2

All the essential data required to address the problem is subsequently gathered. Similar to the majority of multi-criteria decision analysis methodologies, the inputs consist of alternatives, criteria, the weights assigned to each criterion (w_j), and the ratings (x_{ij}) associated with each alternative Ai concerning criterion Cj.

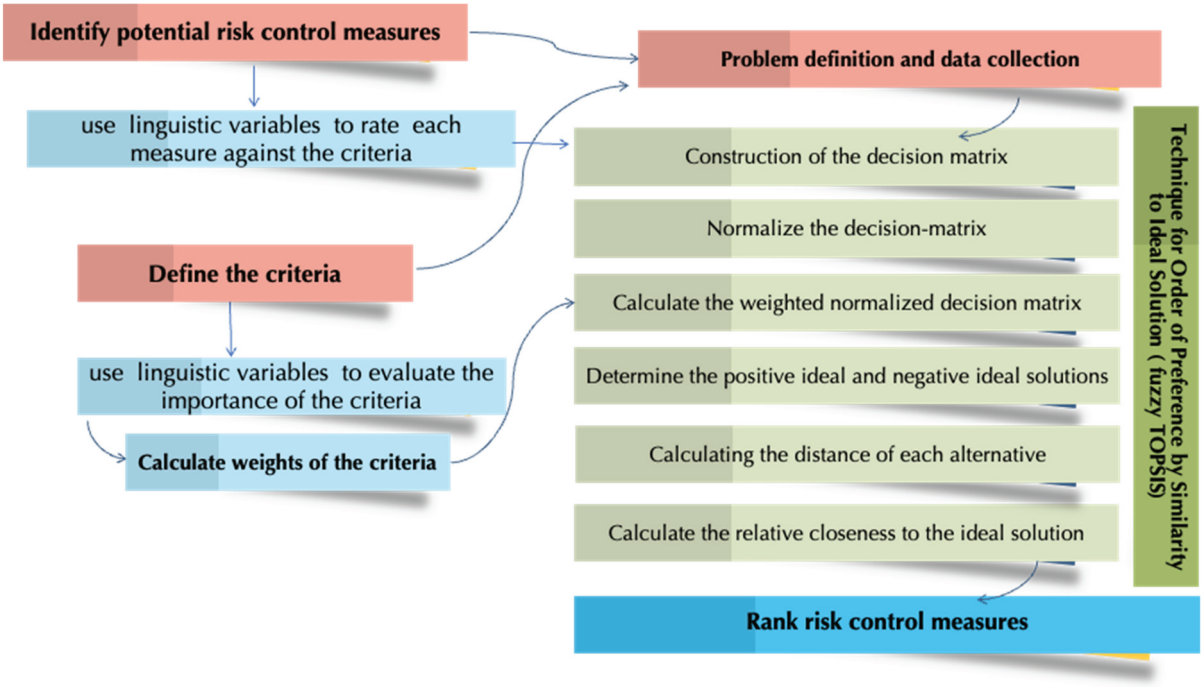

Figure 2. The fuzzy TOPSIS methodology employed in this study.

Aggregation of the weights of the criteria

The importance of each criterion can be obtained by different methods, for example, by direct assignment or indirectly using pairwise comparisons, which is commonly used in the Analytic Hierarchy Process (AHP) method. In this work, and in line with Chen (2000), a group of experts provides their opinion on the importance of each criterion using linguistic variables represented as triangular fuzzy numbers; see definitions in Table B1 (Appendix B).

Assuming a group of K decision makers (or experts), the importance of each criterion can be calculated as the average:

$$\tilde{w}_j = \frac{1}{K}\left[\tilde{w}_j^1 \oplus \tilde{w}_j^2 \oplus \ldots \oplus \tilde{w}_j^K\right] \tag{1}$$

where $\tilde{w}_j^K$ is the importance weight (represented as a fuzzy triangular number) of the K-th decision-maker.

Aggregation of the ratings

We, then, ask the experts to provide their ratings using the linguistic terms presented in Table B2 (Appendix B). Assuming K experts (or decision makers), the rating of alternatives with respect to each criterion can be calculated as follows:

$$\tilde{x}_{ij} = \frac{1}{K}\left[\tilde{x}_{ij}^1 \oplus \tilde{x}_{ij}^2 \oplus \ldots \oplus \tilde{x}_{ij}^K\right] \tag{2}$$

where $\tilde{x}_{ij}^k$ is the rating of the kth decision maker (represented as a fuzzy triangular number) for alternative A_i with respect to criterion C_j.

Step 2. Construction of the decision matrix

The fuzzy multicriteria group decision-making problem can then be expressed as follows:

$$\widetilde{D} = C_1 C_2 \ldots C_n A_1 A_2 \vdots A_m \left[\tilde{x}_{11}\tilde{x}_{12}\tilde{x}_{21}\tilde{x}_{22}\ldots\tilde{x}_{1n}\ldots\tilde{x}_{2n}\vdots\vdots\tilde{x}_{m1}\tilde{x}_{m2}\vdots\vdots\vdots\tilde{x}_{mn}\right], i = 1,2,\ldots,m; j = 1,2,\ldots,n \tag{3}$$

where $A_1, A_2, \ldots, A_m$ are the alternatives, $C_1, C_2, \ldots, C_n$ the criteria, and x_{ij} the fuzzy numbers that indicate the rating of the alternative A_i with respect to criterion C_j.

Step 3. Normalisation of the decision matrix

The inputs are usually normalised to eliminate deviations when using different measurement units and scales. Normalisation is the operation that makes these scores/ratings conform to, or reduce to, normalised values, which are positive values between 0 and 1. In our work, the linear scale transformation is used.

The normalised fuzzy decision matrix is denoted by $\tilde{R}$ can therefore be calculated as follows:

$$\tilde{R} = \left[\tilde{r}_{ij}\right]_{m\times n} \tag{4}$$

where B and C are the set of benefit criteria and cost criteria, respectively, and

$$\tilde{r}_{ij} = \left(\frac{a_{ij}}{c_j^*}, \frac{b_{ij}}{c_j^*}, \frac{c_{ij}}{c_j^*}\right), j \in B \tilde{r}_{ij} = \left(\frac{a_j^-}{c_{ij}}, \frac{a_j^-}{b_{ij}}, \frac{a_j^-}{a_{ij}}\right), j \in C c_j^* = \max_i c_{ij} if j \in B a_j^- = \min_i a_{ij} if j \in C.$$

Step 4. Construction of the weighted normalised decision matrix

The weighted normalised decision matrix $P = \left[p_{ij}\right]_{mxn}$ with $i = 1, \ldots, m$, and $j = 1, \ldots, n$ is then calculated by multiplying the normalised decision matrix by its associated (fuzzy) weights.

The weighted fuzzy normalised value p_{ij} is calculated as:

$$\tilde{p_{ij}} = w_i \tilde{x}_{ij} \text{ with } i = 1, \ldots, m \text{ and } j = 1, \ldots, n$$

Step 5. Calculating the positive and negative ideal solution

The PIS A^+(benefits) and NIS A^-(costs) are calculated as follows:

$$A^+ = (\tilde{p}_1^+, \tilde{p}_2^+, \ldots, \tilde{p}_m^+)$$

$$A^- = (\tilde{p}_1^-, \tilde{p}_2^-, \ldots, \tilde{p}_m^-)$$

where $\tilde{p}_j^+ = (1,1,1)$ and $\tilde{p}_j^- = (0,0,0), j = 1, 2, \ldots, n$.

Step 6. Calculating the distance of each alternative

In this step, the distance of each alternative A_i from the PIS A^+ and the NIS A^-, respectively, are calculated as follows:

$$d_i^+ = \sum_{j=1}^{n} d(\tilde{p}_{ij}, \tilde{p}_j+) \text{with } i = 1, \ldots, m \tag{5}$$

$$d_i^- = \sum_{j=1}^{n} d(\tilde{p}_{ij}, \tilde{p}_j-), \text{with } i = 1, \ldots, m \tag{6}$$

where the distance $d\left(\tilde{p}_{ij}, \tilde{p}_j^+\right)$ is defined in Definition 4 (Appendix B).

Step 7. Calculating the relative closeness to the ideal solution and scoring the alternatives

The last step is to calculate the relative closeness ξ_i for each alternative A_i with respect to the PIS using the formula below:

$$\xi_i = \frac{d_i^-}{d_i^+ + d_i^-} \tag{7}$$

The alternatives are ranked according to their relative closeness. The best alternatives are those that have higher value ξ_i and therefore should be chosen because they are closer to the PIS.

Questionnaire design, analysis, and results

Data collection

Data have been obtained using an online questionnaire with three sections. The first section asks the respondents to provide information regarding their work experience and the type of company they are working in. In the second section, the experts were asked to provide their opinions on the importance of

each criterion for the selection of cybersecurity RCMs to address cyber-attacks. In the final section, we elicited the respondents' ratings regarding the seven identified measures, using seven linguistic terms (from very poor to very good) that present the question related to the rating of the alternatives with respect to their effectiveness in reducing the "Likelihood" of cyber-attacks.

Selecting the right participants for a questionnaire, especially when seeking expert opinions, is crucial for obtaining valuable and reliable data. We utilised non-probability sampling methods, starting with a "purposeful sampling" (also known as judgment or subjective sampling), relying on our own judgment when choosing members of the population to participate in the study. This method involved selecting participants based on their expertise or knowledge in the specific field, but who are also easy to reach and willing to participate. In order to obtain a high number of responses, we asked these experts to recommend other experts they know, creating a snowball effect – this is known as "snowball sampling."

To mitigate potential biases, several methodological safeguards were incorporated throughout the research process. Although explicit eligibility requirements were not formally predefined, the research team directly selected an initial group of verified experts based on their demonstrable professional experience and relevance to the maritime sector. Verification was carried out through publicly available professional information, such as organizational affiliations or published records. By inviting these verified experts to recommend additional qualified individuals, we ensured that subsequent participants were also likely to possess genuine expertise, thereby reducing the likelihood of unqualified respondents influencing the results.

Furthermore, efforts were made to include experts representing a range of professional roles and backgrounds to prevent dominance by any particular subgroup. This diversity of perspectives strengthened the robustness and representativeness of the findings, as further discussed in the concluding section. To maintain data integrity, responses exhibiting uniform ratings (for example, identical scores across all items) or extreme outliers inconsistent with overall response patterns were excluded during the screening stage. To confirm that these exclusions did not affect the analytical outcomes, a sensitivity analysis was performed in which all responses were retained; the resulting rankings remained consistent, thereby supporting the reliability and stability of the results.

Profile of the respondents

A total of 105 responses have been received, of which 100 were used in analysis. Five responses were unsuitable, as they provided, for example, uniform answers, i.e., they provided the same rating for all alternatives, or others provided scores that were extreme compared to the average values.

For validation, the analysis was repeated without removing outliers, and the resulting rankings remained consistent. Preliminary analyses also produced similar results across different respondent groups and under alternative inclusion criteria, such as varying lengths of professional experience. As noted in the Conclusions, a promising direction for future research would be to compare rankings across stakeholder categories – such as seafarers, ship operators, policymakers, or experts from different age groups – to explore potential differences in perspectives, particularly regarding familiarity with modern information technologies.

Table 1 presents their profiles. Over 50% of them are from shipping companies (including owners, operators, and seafarers), and over 70% of them have more than 5 years of experience working in the maritime industry.

Table 1. Respondents' background.

Organisation	Shipping companies	52
	Port operator	6
	Regulator	5
	Academia	24
	Other (incl. Class, spares, associations)	13
Work experience	Less than 5 years	21
	6–10 years	23
	11–15 years	13
	More than 15 years	38
	No response	5

Results

The expert opinions regarding the weights and the rates have been aggregated using simple means per the classical approach of Chen (2000); see Equation 1 and Equation 2

Weights of criteria

The weights are presented as fuzzy triangular numbers; their crisp values using the so-called graded mean integration are also presented for illustrative reasons (see Table 2). Based on the responders' opinion the most important criteria in the selection of the most appropriate measures are "reliability," and the FMEA-inspired "effectiveness in reducing the likelihood" and "effectiveness in reducing the severity", respectively.

Rank of alternatives

The resulting decision matrix is shown in Table C2 (Appendix C). This decision matrix and the fuzzy weights are the main inputs to the fuzzy TOPSIS methodology presented in Section 3. Table C3 presents the weighted normalised matrix. Finally, the relative closeness to the ideal solutions has been calculated, and alternatives were ranked based on this relative closeness value; see Table 3.

Based on the above results, the experts believe that the best approach (alternative/strategy) to mitigate the risk of cyberattacks is "Effective Antivirus software management" (A2), followed by "Management of network devices" (A5) and "Developing a cybersecurity strategy" (A7).

Note that the results of all MCDM methods (including ours) are sensitive to the weights used and the methodology used. In the classical approach, a sensitivity analysis is usually presented; this is straightforward in the classical TOPSIS, where weights can slightly be changed to investigate the impact of changes in the final rankings. In our case, and in line with similar studies such as Yan et al. (2017) and Emovon and Aibuedefe (2020), a validation is performed by comparing our results with those obtained using similar methods such as Fuzzy VIKOR (VIseKriterijumska Optimizacija I Kompromisno Resenje) and Fuzzy Weighted Aggregated Sum Product ASsessment (Fuzzy WASPAS); see Table C4 (Appendix C) for more details. As it can be seen, all methods agree that A2 and A5 are the top measures to address cybersecurity risks. Possible limitations of the approach are discussed in Section 6.1, but based on the above validation process, the results are robust.

In the next section, we offer some views on how these strategies could be implemented to make maritime systems more cyber secure.

Discussion and practical implications

To begin with, it comes as no surprise that the stakeholders feel that the third most important measure to control the relevant risks is the development of a cybersecurity strategy. BIMCO guidelines (BIMCO, 2020) were indeed introduced to *"assist in the development of a proper cyber risk management strategy in accordance with relevant regulations and best practises on board a ship with a focus on work processes,*

Table 2. Weights of criteria.

	Reliability	Economic Affordability	Ease of use	Reducing Likelihood	Reducing Severity	Reducing Undetectability
Fuzzy Weights	(0.77,0.91,0.96)	(0.52,0.69,0.82)	(0.57,0.74,0.88)	(0.71,0.87,0.95)	(0.72,0.87,0.95)	(0.67,0.83,0.93)
Crisp values	0.1843	0.1405	0.1519	0.1769	0.1771	0.1693

Table 3. Relative closeness to the ideal solutions and score of the alternatives.

	A1	A2	A3	A4	A5	A6	A7
Distance from PIS	2.465	2.144	2.307	2.301	2.293	2.394	2.286
Distance from NIS	3.948	4.296	4.161	4.135	4.168	4.051	4.152
Relative closeness	0.616	0.667	0.643	0.642	0.645	0.629	0.645
Rank	7	**1**	4	5	**2**	6	**3**

Legend: A1 Education and training; A2 Effective Antivirus software management; A3 Hardware and software maintenance; A4 Strong password policy; A5 Personal device management; A6 Management of network devices; A7 Developing a cybersecurity strategy.

equipment, training, incident response and recovery management." The need for a risk-based approach to managing risk is here expected; and indeed, many of the relevant studies, both academic and those in the "grey literature," are in this area. Not to forget that there is an expectation of stakeholders to comply with the relevant regulations. In fact, according to IMO Resolution MSC.428 (98), ship owners and managers are obligated to evaluate cyber risk and implement relevant measures across all facets of their safety management system, which is incorporated within the International Safety Management Code (ISM). Furthermore, it's important to note that the IMO introduced the "Guidelines on Maritime Cyber Risk Management" (refer to IMO document MSC-FAL.1/Circ.3/Rev.2) in June 2022. However, both of these documents leave a considerable amount of interpretation to be carried out by the shipping companies, and based on findings from the literature survey, it is evident that there are still numerous uncertainties regarding how to address these requirements.

Nevertheless, the results are clear; more must be done to make software and hardware systems more secure. Some measures are effective, easy to implement, and not expensive: "use an antivirus," "patch your systems," "apply the latest software updates." As mentioned in Section 2.3 a number of incidents were a result of the failure of software maintenance and patching of systems. There are many systems (software) vulnerabilities that are discovered by attackers even before the vendors are aware of them, these are known as "zero-day vulnerabilities." Not much can be done about these attacks through software updates and patches, but then perhaps a good approach is to better control the network devices and prevent unauthorised access from systems outside the network, for example, using firewalls. A firewall is a network security device that monitors and filters all network traffic (i.e., incoming and outgoing) and it can act as a barrier between the internal network and the "outside world." BIMCO guidelines indeed emphasise the importance of proper configuration of network devices such as firewalls, routers, and switches. According to the BIMCO Guidelines, it is crucial to emphasise the importance of real-time monitoring and response to cyber threats to maintain the operational resilience of shipping activities. In our dynamic world, real-time monitoring is essential and can be achieved using firewalls, routers, and anti-virus and anti-malware solutions, as described below.

Meanwhile, anti-virus and anti-malware software packages are inexpensive solutions that detect viruses and malware in real-time and quarantine them so that they cannot cause any damage. Humans do not necessarily, even if trained, pay much attention when downloading software or files from unfamiliar or unreliable sources. Email viruses are also becoming increasingly popular; malicious code is distributed in email messages and when activated it can infect the devices. Therefore, while email attachments are deemed to be a popular and convenient way to send and share files, they are also a very common source of viruses. Anti-virus software is, therefore, very important in preventing the downloading and executing of malicious code. Nowadays, antivirus solutions often offer "total protection" such as virus and malware protection, including extra features like anti-phishing, virtual private networks (VPN) solutions and firewalls. In this sense, it is not surprising that based on the stakeholders' opinion, this is the most effective solution to deal with cybersecurity risks.

Policy and practical implications

Based on the above analysis, we propose the following recommendations to be considered by the maritime industry and the regulators.

In the short term, the industry should prioritise investment in hardware and software as they can effectively and efficiently reduce the likelihood and the consequences of the equipment being cyber-attacked. For example, although the "Bring Your Own Device (BYOD)" policy has several significant advantages (e.g., cost savings for companies, reduced needs for IT training, etc.), these personal devices are easier to attack compared to company managed devices. Companies could implement several strategies to enhance cybersecurity in the short term, some of them are quite straightforward to implement. We suggest purchasing and offering employees (also for their personal devices) comprehensive antivirus software. This is the most effective way to prevent malicious cyber risks from outside of the company, as well as data breaches from inside the company. In addition, we suggest implementing personal device management (e.g., restricting the individual's devices to access the company's sensitive data) and developing a cybersecurity strategy (e.g., providing a guideline for sea crews and staff to be

easy to follow to reduce the likelihood of being cyberattacked and to mitigate the impacts once being cyberattacked). By implementing the above, companies can enjoy the advantages of BYOD, but also mitigate the cyber risks. At the same time, although implementing a strong password policy ranks fifth in our research, it cannot be denied that it is still a very effective and affordable way to address cybersecurity risks. Meanwhile, IMO Member-States should also urge the maritime industry to more strictly implement the "Guidelines on Maritime Cyber Risk Management" proposed by the IMO to prevent and mitigate the impact of cyber risks on the maritime industry. Relevant inspections could take place by the Port State Control (PSC).

Although "*Education and training*" was ranked at the bottom in this research, without doubt, it is very important. A possible explanation is that the responders feel that this would be addressed by having a comprehensive strategy, which would necessarily include an element of training. The maritime industry should keep educating and training staff and crews in order to better understand the importance of cybersecurity and to enhance their cybersecurity awareness. The maritime industry could collaborate with higher education providers and/or maritime related associations, which help to educate and train crews and staff for the industry. The government could also recommend cybersecurity training, as well as offer recognised certificates to encourage more seafarers and staff to take the training (Kanwal et al., 2022).

Conclusion, limitations, and future work

This paper presented the results of a research study to evaluate cybersecurity RCMs based on the stakeholders' opinions. To accomplish this, data was collected through a questionnaire and 100 replies were used as input to apply a Fuzzy TOPSIS method. A key result of our analysis is the following overall performance rank of cybersecurity RCMs in decreasing order: "Effective Antivirus software management," "Hardware and software maintenance" and "Developing a cybersecurity strategy" in terms of six criteria. Based on the above results, we have proposed a number of short- and long-term recommendations to the maritime industry and the regulators to foster the development of maritime cybersecurity. Furthermore, the new methodology can support stakeholders to conduct individual research to choose the best-fit RCM(s) against their own security and cost concerns.

Methodology-wise, a number of possible extensions could be investigated; these are mainly related to the normalisation step and the distance measures used in the TOPSIS approach. Normalisation (see Step 3 of the process) is a fundamental step in all MCDM methods; using different methods (i.e., linear, logarithmic, Markovic, Tzeng and Huang method) and comparing the results could be a suggestion for future research. In addition, the final rank depends on the distance of each alternative from the PIS and NIS; the selected distance metric is therefore of paramount importance. The classical approach for group fuzzy TOPSIS (Chen, 2000) calculates the Euclidean distances; other approaches (such as the Manhattan or Tchebycheff distance) could be investigated; see Ploskas and Papathanasiou (2019) for the alternative approaches.

Sensitivity analysis could also be performed to test the impact of slight variations of the inputs to the final rank; for example, the impact of different weights. Performing a sensitivity analysis in a fuzzy environment is rather challenging, given that the weights are fuzzy and not crisp numbers. Instead, to validate the findings and use the selected method, we used the same input data in various established MCDM methods such as Fuzzy VIKOR, Fuzzy WASPAS and Fuzzy Multi-Objective Optimisation by Ratio Analysis (MOORA). It is out of the scope of this paper to discuss these methods (see Ceballos et al., 2017) for a comparison of these approaches. However, as can be seen in Table C4 (Appendix C), all the methods produced similar ranks for our input data. This is an interesting result, which shows that our results are robust. This means that using other methods would indeed render similar results and our managerial/policy implications would, therefore, still be valid.

The important areas for future investigation are the different criteria to be used and, most importantly, the measures to be assessed. In this study, the RCMs are expressed in broad terms to stimulate a widespread application as well as to address the uncertainty in data on the specific RCMs. There is, however, a need for more application-specific control measures, perhaps also identifying the prevention and recovery options through a more systematic approach, for example, using Bow-tie analysis, Hazard & Operability Analysis (HAZOP), etc. In addition, the RCMs can focus on specific ship types and segments, or particular sectors of the maritime industry. According to Tonn et al. (2019),

very few studies focus specifically on cyber risk in the transportation infrastructure industry; maritime ports are very vulnerable and could be the focus of dedicated studies using our proposed methodology.

Another interesting area would also be to compare the findings, i.e., the ranks for different stakeholders to identify differences in the perspectives of, say, the seafarers and ship operators or policymakers, or between experts coming from different countries, or different age groups (assuming here that younger responders could be more familiar with modern information technologies). This will help stimulate the development of the compromising policies that can be best accepted by all stakeholders and hence easier for their implementation.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

The work was supported by the HORIZON EUROPE European Research Council [864724]; Royal Society [IEC\NSFC\223196].

ORCID

Chia-Hsun Chang http://orcid.org/0000-0002-7351-8471

Data availability statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

References

Alcaide, J. I., & Llave, R. G. (2020). Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia*, *45*, 547–554. https://doi.org/10.1016/j.trpro.2020.03.058

Alzahrani, A., Petri, I., Rezgui, Y., & Ghoroghi, A. (2021). Decarbonisation of seaports: A review and directions for future research. *Energy Strategy Reviews*, *38*, 100727. https://doi.org/10.1016/j.esr.2021.100727

Ashraf, I., Park, Y., Hur, S., Kim, S. W., Alroobaea, R., Zikria, Y. B., & Nosheen, S. (2022). A survey on cyber security threats in IoT-enabled maritime industry. *IEEE Transactions on Intelligent Transportation Systems*, *24*(2), 2677–2690.

Behzadian, M., Otaghsara, S. K., Yazdani, M., & Ignatius, J. (2012). A state-of the-art survey of TOPSIS applications. *Expert Systems with Applications*, *39*(17), 13051–13069. https://doi.org/10.1016/j.eswa.2012.05.056

Belabyad, M., Kontovas, C., Pyne, R., Shi, W., Li, N., Szwed, P., & Chang, C. H. (2025). The human element in autonomous shipping: A study on skills and competency requirements. *WMU Journal of Maritime Affairs*, 1–31. https://doi.org/10.1007/s13437-025-00366-9

BIMCO. (2016). *The guidelines on cyber security onboard ships*. https://www.maritimeglobalsecurity.org/media/1014/c-users-jpl-onedrive-bimco-desktop-guidelines_on_cyber_security_onboard_ships_version_2-0_july2017.pdf

BIMCO. (2018). The guidelines on cyber security onboard ships https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

BIMCO. (2020). The guidelines on cyber security onboard ships. https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

Bolbot, V., Kulkarni, K., Brunou, P., Banda, O. V., & Musharraf, M. (2022). Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. *International Journal of Critical Infrastructure Protection*, *39*, 100571. https://doi.org/10.1016/j.ijcip.2022.100571

Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D. (2020). A novel cyber-risk assessment method for ship systems. *Safety Science*, *131*, 104908. https://doi.org/10.1016/j.ssci.2020.104908

Boyes, H., & Isbell, R. (2017). *Code of practice: Cyber security for ships*. Institution of Engineering and Technology.

Canepa, M., Ballini, F., Dalaklis, D., & Vakili, S. (2021). Assessing the effectiveness of cybersecurity training and raising awareness within the maritime domain. In *INTED2021 Proceedings*, (pp. 3489-3499). IATED doi:10.21125/inted.2021.0726.

Cao, Y., Wang, X., Yang, Z., Wang, J., Wang, H., & Liu, Z. (2023). Research in marine accidents: A bibliometric analysis, systematic review and future directions. *Ocean Engineering*, *284*, 115048. https://doi.org/10.1016/j.oceaneng.2023.115048

Ceballos, B., Lamata, M. T., & Pelta, D. A. (2017). Fuzzy multicriteria decision-making methods: A comparative analysis. *International Journal of Intelligent Systems*, *32*(7), 722–738. https://doi.org/10.1002/int.21873

Chan, H. L., & Choi, T. M. (2023). Logistics management for the future: The IJLRA framework. *International Journal of Logistics Research and Applications*, *27*(12), 2466–2484.

Chang, C. H., Kontovas, C., Yu, Q., & Yang, Z. (2021). Risk assessment of the operations of maritime autonomous surface ships. *Reliability Engineering & System Safety*, *207*, 107324. https://doi.org/10.1016/j.ress.2020.107324

Chang, C. H., Wenming, S., Wei, Z., Changki, P., & Kontovas, C. (2019). Evaluating cybersecurity risks in the maritime industry: A literature review. In *Proceedings of the International Association of Maritime Universities (IAMU) conference*.

Chen, C. T. (2000). Extensions of the TOPSIS for group decision-making under fuzzy environment. *Fuzzy Sets and Systems*, *114*(1), 1–9. https://doi.org/10.1016/S0165-0114(97)00377-1

Chukwuka, O. J., Ren, J., Wang, J., & Paraskevadakis, D. (2024). Managing risk in emergency supply chains-an empirical study. *International Journal of Logistics Research and Applications*, *28*(9), 1–37. https://doi.org/10.1080/13675567.2024.2359645

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the industrial internet of things: A systematic literature review. *Computers in Industry*, *137*, 103614. https://doi.org/10.1016/j.compind.2022.103614

Dağdeviren, M., Yavuz, S., & Kılınç, N. (2009). Weapon selection using the AHP and TOPSIS methods under fuzzy environment. *Expert Systems with Applications*, *36*(4), 8143–8151. https://doi.org/10.1016/j.eswa.2008.10.016

De la Peña Zarzuelo, I. (2021). Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue. *Transport Policy*, *100*, 1–4. https://doi.org/10.1016/j.tranpol.2020.10.001

Dellios, K., & Papanikas, D. (2014). Deploying a maritime cloud. *IT Professional*, *16*(5), 56–61.

Drazovich, L., Brew, L., & Wetzel, S. (2021). Advancing the state of maritime cybersecurity guidelines to improve the resilience of the maritime transportation system. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 503-509). doi:10.1109/CSR51186.2021.9527922.

Emovon, I., & Aibuedefe, W. O. (2020). Fuzzy TOPSIS application in materials analysis for economic production of cashew juice extractor. *Fuzzy Information and Engineering*, *12*(1), 1–18. https://doi.org/10.1080/16168658.2020.1775332

Fan, S., & Yang, Z. (2022). Safety and security co-analysis in transport systems: Current state and regulatory development. *Transportation Research Part A: Policy and Practice*, *166*, 369–388. https://doi.org/10.1016/j.tra.2022.11.005

Fischer-Hübner, S., Alcaraz, C., Ferreira, A., Fernandez-Gago, C., Lopez, J., Markatos, E., Islami, L., & Akil, M. (2021). Stakeholder perspectives and requirements on cybersecurity in Europe. *Journal of Information Security and Applications*, *61*, 102916. https://doi.org/10.1016/j.jisa.2021.102916.

Fitton, O., Prince, D., Germond, B., & Lacy, M. (2015). *The future of maritime cyber security*. Lancaster University.

Guanah, J. S. (2021). Mass media and cyber security in the maritime industry: Analysing the threats and prevention. *Global Journal of Arts Humanity and Social Sciences*, *2583*, 63–72. ISSN: 2583-2034.

Hayes, C. R. (2016). Maritime cybersecurity: The future of national security (Doctoral dissertation, Naval Postgraduate School).

Hemminghaus, C., Bauer, J., & Padilla, E. (2021). Brat: A bridge attack tool for cyber security assessments of maritime systems. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, *15*(1), 35–44. https://doi.org/10.12716/1001.15.01.02

Hopcraft, R., & Martin, K. M. (2018). Effective maritime cybersecurity regulation-the case for a cyber code. *Journal of the Indian Ocean Region*, *14*(3), 354–366. https://doi.org/10.1080/19480881.2018.1519056

Hwang, C.-L., Lai, Y.-J., & Liu, T.-Y. (1993). A new approach for multiple objective decision making. *Computers & Operations Research*, *20*(8), 889–899. https://doi.org/10.1016/0305-0548(93)90109-V

Hwang, C.-L., & Yoon, K. (1981). Methods for multiple attribute decision making. In *Multiple attribute decision making* (pp. 58–191). Springer.

IMO. (2017). Guidelines on maritime cyber risk management. Imo document msc-fal.1-circ.3-rev.1, International Maritime Organisation, https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/Facilitation/MSC-FAL.1-Circ.3-Rev.1.pdf

ISO. (2018). Risk management - guideline. ISO 31000: 2018. https://www.iso.org/standard/65694.html

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Jensen, R. B. (2021). Fragmented digital connectivity and security at sea. *Marine Policy*, *130*, 104289. https://doi.org/10.1016/j.marpol.2020.104289

Jones, K. D., Tam, K., & Papadaki, M. (2016). Threats and impacts in maritime cyber security. *Engineering & Technology Reference*, *1*(1), 1–5. https://doi.org/10.1049/etr.2015.0123

Kanwal, K., Shi, W., Kontovas, C., Yang, Z., & Chang, C. H. (2022). Maritime cybersecurity are onboard systems ready? *Maritime Policy & Management*, *51*(3), 1–19. https://doi.org/10.1080/03088839.2022.2124464

Karahalios, H. (2020). Appraisal of a ship's cybersecurity efficiency: The case of piracy. *Journal of Transportation Security*, *13*(3), 179–201. https://doi.org/10.1007/s12198-020-00223-1

Karim, M. S. (2022). Maritime cybersecurity and the IMO legal instruments: Sluggish response to an escalating threat? *Marine Policy*, *143*, 105138. https://doi.org/10.1016/j.marpol.2022.105138.

Knight, V., & Sadok, M. (2021). Is cyber-security the new lifeboat? An exploration of the employee's perspective of cyber-security within the cruise ship industry. In Peter Bednar, Alexander Nolte, Mikko Rajanen, Anna Sigridur Islind, Helena Vallo Hult, Fatema Zaghloul, Aurelio Ravarini, & Alessio Maria Braccini (Eds.), *7th International Workshop on Socio-Technical Perspective in IS Development (STPIS 2021)* (pp. 216–231). CEUR Workshop Proceedings.

Koola, P. M. (2018). Cybersecurity: A deep dive into the abyss. *Marine Technology Society Journal*, *52*(5), 31–43. https://doi.org/10.4031/MTSJ.52.5.2

Kumar, R., Khan, S. A., Alharbe, N., & Khan, R. A. (2024). Code of silence: Cyber security strategies for combating deepfake disinformation. *Computer Fraud & Security*, *2024*(4). https://doi.org/10.12968/S1361-3723(24)70013-X

Kumar, R., Khan, S.A., & Khan, R. A. (2023). *Software durability: Concepts and practices* (1st ed.). CRC Press. https://doi.org/10.1201/9781003322351

Lagouvardou, S. (2018). *Maritime cyber security: Concepts, problems and models*. Kongens Lyngby.

Lee, A. R., & Wogan, H. P. (2018). All at sea: The modern seascape of cybersecurity threats of the maritime industry. In *Oceans, 2018 MTS/IEEE Charleston* (pp. 1–8). IEEE.

Li, Z., & Kang, R. (2015). Strategy for reliability testing and evaluation of cyber physical systems. In *2015 IEEE international conference on industrial engineering and engineering management (IEEM)* (pp. 1001-1006). IEEE. doi:10.1109/IEEM.2015.7385799.

Lin, C. C., Yang, Z., & Chang, C. H. (2022). Facilitating adoption of virtual communities through emotional connection in the global logistics industry. *International Journal of Logistics Research and Applications 28*(2), 191–209. https://doi.org/10.1080/13675567.2022.2153815.

Logan, T. M., Aven, T., Guikema, S. D., & Flage, R. (2022). Risk science offers an integrated approach to resilience. *Nature Sustainability*, *5*(9), 741–748. https://doi.org/10.1038/s41893-022-00893-w

Martín-Duque, C., Romero-Padilla, Y., Babinger, F., & Ruiz-Guerra, I. (2023). Key cooperation strategies between Spanish ports and tourist destinations: An exploratory analysis. *Research in Transportation Business & Management*, *47*, 100942. https://doi.org/10.1016/j.rtbm.2022.100942

Meland, P. H., Bernsmed, K., Wille, E., Rødseth, Ø. J., & Nesheim, D. A. (2021). A retrospective analysis of maritime cyber security incidents. *TransNav*, *15*(3), 519–530. https://doi.org/10.12716/1001.15.03.04

Mohsendokht, M., Li, H., Kontovas, C., Chang, C., Qu, Z., & Yang, Z. (2024). Decoding dependencies among the risk factors influencing maritime cybersecurity: Lessons learned from historical incidents in the past two decades. *Ocean Engineering*, *312*(1), 119078. https://doi.org/10.1016/j.oceaneng.2024.119078

National Cyber Security Centre. (2019). Password policy: Updating your approach. https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

Park, C., Kontovas, C., Yang, Z., & Chang, C. H. (2023). A BN driven FMEA approach to assess maritime cybersecurity risks. *Ocean & Coastal Management*, *235*, 106480. https://doi.org/10.1016/j.ocecoaman.2023.106480

Ploskas, N., & Papathanasiou, J. (2019). A decision support system for multiple criteria alternative ranking using TOPSIS and VIKOR in fuzzy and nonfuzzy environments. *Fuzzy Sets and Systems*, *377*, 1–30. https://doi.org/10.1016/j.fss.2019.01.012

Poghosyan, A., Manu, P., Mahamadu, A. M., Akinade, O., Mahdjoubi, L., Gibb, A., & Behm, M. (2020). A web-based design for occupational safety and health capability maturity indicator. *Safety Science*, *122*, 104516. https://doi.org/10.1016/j.ssci.2019.104516

Progoulakis, I., Rohmeyer, P., & Nikitakos, N. (2021). Cyber physical systems security for maritime assets. *Journal of Marine Science and Engineering*, *9*(12), 1384. https://doi.org/10.3390/jmse9121384

Pseftelis, T., & Chondrokoukis, G. (2021). A study about the role of the human factor in maritime cybersecurity. *Spoudai-Journal of Economics and Business*, *71*(1–2), 55–72.

Sheehan, B., Murphy, F., Mullins, M., & Ryan, C. (2019). Connected and autonomous vehicles: A cyber-risk classification framework. *Transportation Research Part A: Policy and Practice*, *124*, 523–536. https://doi.org/10.1016/j.tra.2018.06.033

Svilicic, B., Kristić, M., Žuškin, S., & Brčić, D. (2020). Paperless ship navigation: Cyber security weaknesses. *Journal of Transportation Security*, *13*(3), 203–214.

Tonn, G. L., Kesan, J. P., Zhang, L., & Czajkowski, J. (2019). Cyber risk and insurance for transportation infrastructure. *Transport Policy*, *79*, 103–114. https://doi.org/10.1016/j.tranpol.2019.04.019

Tyagi, M., Kumar, P., & Kumar, D. (2018). Assessment of CSR based supply chain performance system using an integrated fuzzy AHP-TOPSIS approach. *International Journal of Logistics Research and Applications*, *21*(4), 378–406. https://doi.org/10.1080/13675567.2017.1422707

Wang, Y., Chen, P., Wu, B., Wan, C., & Yang, Z. (2022). A trustable architecture over blockchain to facilitate maritime administration for mass systems. *Reliability Engineering & System Safety*, *219*, 108246.

Wimpenny, G., Šafář, J., Grant, A., & Bransby, M. (2021). Securing the automatic identification system (AIS): Using public key cryptography to prevent spoofing whilst retaining backwards compatibility. *The Journal of Navigation*, *75*(2), 1–13. https://doi.org/10.1017/S0373463321000837

Yan, X. P., Wan, C. P., Zhang, D., & Yang, Z. (2017). Safety management of waterway congestions under dynamic risk conditions-a case study of the Yangtze River. *Applied Soft Computing*, *59*, 115–128. https://doi.org/10.1016/j.asoc.2017.05.053

Yang, C. C., & Hsu, W. L. (2018). Evaluating the impact of security management practices on resilience capability in maritime firms-a relational perspective. *Transportation Research Part A: Policy and Practice*, *110*, 220–233. https://doi.org/10.1016/j.tra.2017.06.005

Yang, Z., Bonsall, S., & Wang, J. (2008). Fuzzy rule-based Bayesian reasoning approach for prioritization of failures in FMEA. *IEEE Transactions on Reliability*, *57*(3), 517–528.

Yang, Z., & Wang, J. (2015). Use of fuzzy risk assessment in FMEA of offshore engineering systems. *Ocean Engineering*, *95*, 195–204. https://doi.org/10.1016/j.oceaneng.2014.11.037

Yeo, S., Jeong, B., & Lee, W. J. (2023). Improved formal safety assessment methodology using fuzzy TOPSIS for LPG-fueled marine engine system. *Ocean Engineering*, *269*, 113536. https://doi.org/10.1016/j.oceaneng.2022.113536

Yoo, Y., & Park, H.-S. (2021). Qualitative risk assessment of cybersecurity and development of vulnerability enhancement plans in consideration of digitalized ship. *Journal of Marine Science and Engineering*, *9*(6), 565. https://doi.org/10.3390/jmse9060565

Zhang, M., Zhang, D., Yao, H., & Zhang, K. (2020). A probabilistic model of human error assessment for autonomous cargo ships focusing on human-autonomy collaboration. *Safety Science*, *130*, 104838. https://doi.org/10.1016/j.ssci.2020.104838

Zhang, X., & Lam, J. S. L. (2019). A fuzzy delphi-AHP-TOPSIS framework to identify barriers in big data analytics adoption: Case of maritime organizations. *Maritime Policy & Management*, *46*(7), 781–801. https://doi.org/10.1080/03088839.2019.1628318

Appendices

Appendix A Maritime cyberattack incidents from 2019 to 2023

Year	Organisation	Description
2019	U.S merchant ship	The US Coast Guard has reported that malware attacks had a significant effect of degrading the function of the onboard control system network.
2019	James Fisher & Sons	UK-based Marine service provider company informed that its computer systems had suffered an unauthorised intrusion. They disconnected from communication and financial systems while they recovered.
2019–2020	Carnival Corporation & plc	Carnival Corporation & plc, a cruise operator, has suffered two ransomware attacks in two years, resulting in the theft of personal information and credit card details of customers and employees. The details of the virus and mode of attack have not been disclosed, but the company has warned of potential compensation claims from affected parties.
2020	CMA-CGM	The network system was cyberattacked by ransomware. To deal with such attacks, CMA-CGM blocked their e-commerce website to protect customers.
2020	IMO	The website and intranet were attacked by a sophisticated cyberattack suspected of being ransomware. This caused limited access until systems were recovered.
2020	MSC	MSC, a shipping company based in Geneva, Switzerland, suffered an attack by a ransomware virus, resulting in the closure of its headquarters for a period of five days.
2020	Matson shipping company	Matson, a transportation and shipping company based in the United States, has reported a system outage caused by a cyberattack. While the attack has not disrupted cargo operations, certain transactions have been delayed as the affected functions need to be manually processed.
2020	Port of Kennewick	The IT systems of the Port of Kennewick were rendered unusable by a ransomware attack, following which the hackers demanded a ransom of 200,000 USD. However, the ransom was not paid, and the systems remained unavailable for several days until they could be restored from offline backups.
2020	Hurtigruten cruise	Hurtigruten, a Norwegian cruise operator, experienced a significant ransomware attack that had a severe impact on its IT infrastructure, resulting in the unavailability of multiple critical systems for several days. The incident also led to the exposure of passenger data, including passport information, which may have been compromised.
2020	AIDA cruise	AIDA, a German cruise operator based in Rostock, suffered an attack by the DoppelPaymer ransomware, which led to significant IT issues, ultimately forcing the company to cancel a number of scheduled cruises.
2021	Transnet	The online system of this South African container terminal operator was cyberattacked, which caused data and financial.
2021	Greek shipping companies	Several Greek shipping companies suffered a ransomware attack in 2021 that spread through the systems of an IT consulting firm.
2022	European oil port terminal	Oil loading facilities in Germany and spread to key terminals in the Amsterdam-Rotterdam-Antwerp network. There was a cyberattack at various terminals, and quite some terminals were disrupted due to their software being suffered and the operational system being down.
2022	Port of Lisbon	Port of Lisbon's website and international computer system has been shut down due to a cyberattack. Hacker groups announced that vital port-related data are stolen, such as financial reports, audits, budgets, contracts, cargo information etc.
2023	DNV	DNV has found that their Ship Manager software was attacked by hackers. Therefore, Ship Manager's IT server has been shut down. However, there is any damage to data and other software yet.

Appendix B Fuzzy Theory and basic arithmetic

Fuzzy models, for example, using triangular fuzzy numbers, have been used very effectively in solving decision-making problems where the available information is imprecise. Below, we provide some basic definitions of fuzzy sets and fuzzy arithmetic based onDağdeviren et al. (2009).

Definition 1. A fuzzy set $\tilde{A}$ in a universe of discourse X is characterised by a membership function $\mu_A(x)$ that assigns a real number in the interval $[0;1]$ to each element x. The value $\mu_A(x)$ is termed the grade of membership of x in $\tilde{A}$.

Definition 2. A triangular fuzzy number a is defined by a triplet $a = (a_1, a_2, a_3)$ as shown in Figure B1.

The membership function is defined as follows:

$$\mu_a(x) = \{0, x\left\langle a_1 \frac{x-a_1}{a_2-a_1}, a_2 x a_1 \frac{x-a_2}{a_3-a_2}, a_3 x a_2 0, x\right\rangle a_3$$

where a_2 represents the value for which $\mu_a(a_2) = 1$, and a_1 and a_3 are the most extreme values on the left and on the right of the fuzzy number a, respectively, with membership $\mu_a(a_1) = \mu_a(a_3) = 0$; as per Figure B1.

Definition 3. Some main operations (such as addition, subtraction, multiplication and division, etc.) of positive fuzzy numbers $a = (a_1, a_2, a_3)$ and $b = (b_1, b_2, b_3)$ can be expressed as follows:

$$\tilde{D} = C_1 C_2 \ldots C_n A_1 A_2 \vdots A_m \left[\tilde{x}_{11} \tilde{x}_{12} \tilde{x}_{21} \tilde{x}_{22} \ldots \tilde{x}_{1n} \ldots \tilde{x}_{2n} \vdots\vdots \tilde{x}_{m1} \tilde{x}_{m2} \vdots\vdots\vdots \tilde{x}_{mn} \right], i = 1, 2, \ldots, m; j = 1, 2, \ldots, n$$

Definition 4. Be two triangular fuzzy numbers $a = (a_1, a_2, a_3)$ and $b = (b_1, b_2, b_3)$ then the (Euclidean) distance between them is calculated by:

$$d(a, b) = \sqrt{\frac{1}{3}\left[(a_1 - b_1)^2 + (a_2 - b_2)^2 + (a_3 - b_3)^2\right]}$$

Linguistic variables (per Chen, 2000)

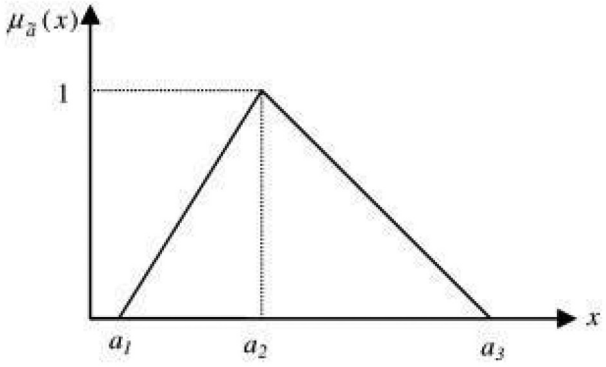

Figure B1. Triangular fuzzy number.

Table B1. Linguistic variables for the importance weight of each criterion.

Linguistic Variable	Fuzzy number
Very low (VL)	(0, 0, 0.1)
Low (L)	(0, 0.1, 0.3)
Medium low (ML)	(0.1, 0.3, 0.5)
Medium (M)	(0.3, 0.5, 0.7)
Medium high (MH)	(0.5, 0.7, 0.9)
High (H)	(0.7, 0.9, 1)
Very high (VH)	(0.9, 1, 1)

Table B2. Linguistic variables for the ratings.

Linguistic Variable	Fuzzy number
Very Poor (VP)	(0, 0, 1)
Poor (P)	(0, 1, 3)
Medium Poor (MP)	(1, 3, 5)
Fair (F)	(3, 5, 7)
Medium Good (MG)	(5, 7, 9)
Good (G)	(7, 9, 10)
Very Good (VG)	(9, 10, 10)

Appendix C Detailed Results

Table C1. Weights.

	RELIABILITY	ECONOMIC AFFORDABILITY	EASE OF USE	Reducing LIKELIHOOD	Reducing SEVERITY	Reducing UNDETECTABILITY
Fuzzy Weights	(0.77,0.91,0.96)	(0.52,0.69,0.82)	(0.57,0.74,0.88)	(0.71,0.87,0.95)	(0.72,0.87,0.95)	(0.67,0.83,0.93)
Crisp values	0.184	0.141	0.152	0.177	0.177	0.169

Table C2. Decision matrix.

	RELIABILITY	ECONOMIC AFFORDABILITY	EASE OF USE	Reducing LIKELIHOOD	Reducing SEVERITY	Reducing UNDETECTABILITY
A1	(6.16,7.84,8.98)	(5.49,7.21,8.50)	(6.13,7.77,8.84)	(5.88,7.55,8.67)	(6.01,7.69,8.83)	(5.61,7.32,8.54)
A2	(7.21,8.74,9.52)	(5.92,7.68,8.87)	(6.08,7.81,8.98)	(7.21,8.74,9.52)	(6.91,8.49,9.35)	(6.95,8.50,9.37)
A3	(6.72,8.44,9.47)	(5.48,7.31,8.68)	(5.19,7.03,8.49)	(6.68,8.41,9.47)	(6.70,8.40,9.42)	(6.40,8.17,9.30)
A4	(6.63,8.29,9.28)	(6.27,7.95,9.03)	(6.07,7.81,9.01)	(6.61,8.25,9.20)	(6.22,7.93,9.05)	(5.94,7.65,8.80)
A5	(6.51,8.21,9.27)	(6.07,7.82,9.01)	(5.57,7.42,8.75)	(6.56,8.30,9.39)	(6.36,8.11,9.23)	(6.48,8.22,9.29)
A6	(6.42,8.19,9.34)	(5.97,7.69,8.86)	(5.70,7.47,8.72)	(6.28,8.04,9.21)	(5.95,7.66,8.88)	(5.76,7.51,8.76)
A7	(6.62,8.27,9.25)	(5.75,7.47,8.69)	(5.75,7.49,8.77)	(6.54,8.21,9.22)	(6.65,8.28,9.24)	(6.58,8.24,9.24)

Table C3. Weighted normalised decision matrix.

	RELIABILITY	ECONOMIC AFFORDABILITY	EASE OF USE	Reducing LIKELIHOOD	Reducing SEVERITY	Reducing UNDETECTABILITY
A1	(0.50,0.75,0.91)	(0.31,0.55,0.78)	(0.39,0.64,0.86)	(0.44,0.69,0.87)	(0.46,0.71,0.89)	(0.40,0.65,0.85)
A2	(0.58,0.83,0.96)	(0.34,0.58,0.81)	(0.38,0.65,0.87)	(0.54,0.80,0.95)	(0.53,0.79,0.94)	(0.49,0.76,0.93)
A3	(0.54,0.81,0.96)	(0.31,0.56,0.79)	(0.33,0.58,0.83)	(0.50,0.77,0.95)	(0.51,0.78,0.95)	(0.45,0.73,0.92)
A4	(0.54,0.79,0.94)	(0.36,0.61,0.82)	(0.38,0.65,0.88)	(0.50,0.75,0.92)	(0.47,0.73,0.91)	(0.42,0.68,0.87)
A5	(0.53,0.78,0.94)	(0.35,0.60,0.82)	(0.35,0.61,0.85)	(0.49,0.76,0.94)	(0.49,0.75,0.93)	(0.46,0.73,0.92)
A6	(0.52,0.78,0.94)	(0.34,0.59,0.81)	(0.36,0.62,0.85)	(0.47,0.74,0.92)	(0.45,0.71,0.90)	(0.41,0.67,0.87)
A7	(0.54,0.79,0.93)	(0.33,0.57,0.79)	(0.36,0.62,0.85)	(0.49,0.75,0.92)	(0.51,0.77,0.93)	(0.47,0.73,0.92)

Table C4. Rank of measures produced by different methods.

Alternatives	MMOORA	TOPSIS (Vector normalisation)	TOPSIS (Linear normalisation)	VIKOR (v = 0.5)	WASPAS (lambda = 0.5)
A1	7	7	7	7	7
A2	1	1	1	1	1
A3	4	3	4	4	3
A4	5	5	5	5	5
A5	2	2	2	3	2
A6	6	6	6	6	6
A7	3	4	3	2	4