Marine Research
of the National Academy of Marine Research
ISSN: 2709-6629 (Vol.1 Iss.1)
GPN: 2011200033

DOI: http://dx.doi.org/10.29677/MR.202112_1(1).0004
2021, 1(1), 59-83

Managing Operational Risks in Container Shipping: A New Approach for the Rising of Information Risk

Son Nguyen [1] Peggy Shu-Ling Chen [1*] Yuquan Du [1]

[1] *National Centre for Ports and Shipping, Australian Maritime College, University of Tasmania, Launceston, Australia*

ABSTRACT

Emerging in parallel with digitalization and automation, information risk is becoming a significant issue with the continuity and effectiveness of container shipping operations. This study conducted a qualitative risk analysis on a database of thirty-two interviewees from container terminal operators, container shipping companies, and freight forwarders. Thematic analysis was applied to shed light on information operational risks (IORs), identifying the ten (10) most typical IORs in container shipping. The pervasiveness of IORs to other container shipping flows was ascertained by realizing their four primary consequences, including delay and unavailability, loss and corruption, leakage and theft, and inaccuracy and manipulation. The study also indicated six factors affecting the IOR situation, reflecting its gaining criticality and uncertainty. Six strategies were recommended for risk mitigation and prevention, focusing on the industry's cyber capability, resilience, interoperability, and transparency. Based on the fundamentals gathered, this study also proposed a new complementary approach to analyze container shipping operational risks considering the pervasiveness and interconnectedness of IORs through a set of four risk parameters and risk causal connections. These results lay the groundwork for an emerging intersection of container shipping risk management and information management – IOR management.

Keywords: Risk analysis, Container shipping, Operational risk, Information management.

* Corresponding author, E mail: p.chen@utas.edu.au

Received 14 September 2021, Accepted 23 November 2021.

1 INTRODUCTION

Container shipping systems are complex cyber-physical systems affected by multiple technical and organizational factors. Container shipping service providers (CSSPs) must to deal with a large range of operational disruptive events (DEs) in information, physical, and payment flows (Tummala and Schoenherr, 2011; Chang et al., 2015). Interdependence of operations along the chain amplifies the consequences toward quality, quantity, and profitability of the container shipping services (Manuj and Mentzer, 2008; Nguyen and Wang, 2018). Among other container shipping operational risks (CSORs), information operational risk (IOR) has been suggested by multiple quantitative risk analyses as gaining momentum to become the most significant category of CSOR (Chang et al., 2015; Nguyen et al., 2019), featuring medium-high likelihood, pervasive potential consequence, and high uncertainty.

These characteristics are observable in the recent large-scale events where the flow of information played a major cause. Explosions and fires due to cargo content misdeclaration in ports and vessels has occurred with higher frequency. Less catastrophic events are cargo handling accidents, high degree rolls, containers overboard, and even capsizing of ships due to weight misdeclarations in combination with heavy weather. In terms of cybersecurity, incidents with large container shipping service providers have been recorded, including the events of Maersk, MSC, COSCO, and Toll Logistics. These events showed the pervasiveness of IORs to physical and payment operations. Meanwhile, influencing factors such as digitalization, new technologies, unstable market sweep across the industry and fuel the uncertainty of IOR's situation (Papathanasiou et al., 2020; Carlan et al., 2020). The complexity and interconnection between DEs pose serious challenges to CSOR analysis, which traditionally treated risks individually. In such conditions, an IOR management's knowledge gap in container shipping is becoming more prominent (Fruth et al., 2017; Chang et al., 2015; Nguyen, 2020).

Risk investigations begin with establishing the contexts of research, in which the perspectives of the risk bearers and the reality of factors affecting risks are studied. This process provides fundamental elements for further analysis, such as characteristics of risk, suitable parameters, and risk qualitative descriptions (Goerlandt and Montewka, 2015b). Empirical studies have proven that these elements play a critical role in quantitative risk analysis results, especially toward the knowledge base where the probability and distribution assessments originate (Goerlandt and Montewka, 2015a; Nguyen, 2020). However, there are still limited dedicated efforts of CSOR studies in this area, causing technical issues in studying risks (e.g., convoluted risk parameters, incomparable risks). Endeavoring to fill this gap, this study uses a qualitative approach to investigate the IOR of the container shipping industry.

Although container shipping involves an extensive range of parties, from service providers, users, and intermediaries to authoritative, governmental, and intergovernmental agencies, this study's intention is not to cover them completely. The objective of the study is to investigate IORs and their potential impacts on other container shipping operations. Therefore, this study focuses on the main actors in transporting containers whose operations involve all three flows of maritime logistics (i.e., information, physical, and payment) (Nguyen et al., 2021b). Telephone interviews were conducted with senior managers in IT, digitalization, innovation, and operation at terminal operators, shipping companies, and freight forwarders to understand their perspectives regarding the current situation of IOR in the industry. Thematic analysis was employed as a tool to analyze the collected qualitative database.

DOI: 10.29677/MR.202112_1(1).0004

For the CSOR and maritime logistics literature, this study erected critical pillars for future research efforts in IOR. Risk descriptions and counter-strategies were presented together with detailed reasonings from the interviewees' experience. The ten identified IORs were explained by six factors and proposed to be addressed using six counter-strategies. These revelations provide an enriched knowledge base for deeper IOR analysis and have opened a view of the upcoming IOR situation of the container shipping industry. Based on those results, this study proposes a new approach to CSOR analysis to address the interconnectedness between IORs and their pervasiveness to other flows.

To the container shipping industry, the identified influencing factors of IORs inform CSSPs in terms of sustainably improving their information management. This study recommends a different approach to CSOR management, in which risks are addressed less individually and more collectively through an in-depth look into the root of the DEs, which increasingly lies in the flow of information. Seeing the whole risk situation through a risk network reveals multiple-event scenarios and create a new risk-countering strategy, where key risk/connections can be identified and addressed to optimize risk mitigation/prevention efforts.

This paper is structured as follows. Section 2 establishes a theoretical basis for IOR qualitative analysis and highlights the research gaps through a literature review. Section 3 introduces our methodology and the demographic features of the participants. Finally, the analysis and interpretation of results are provided in Section 4 before conclusions are drawn in Section 5.

2 LITERATURE REVIEW

The current paper focuses on the intersection of risk management and container shipping operation. Not only does this section provide an overview of the state of the art, it also establishes the theoretical framework for the study with preliminary concepts and methods in use.

2.1 Qualitative risk description

Container shipping systems are cyber-physical systems operating based on the synchronization and cooperation of multiple flows (Ho et al., 2015; Chang et al., 2015). CSORs are multidisciplinary and, therefore, require a holistic concept of risk that can be applied for operational risks in multiple fields, such as information and communication, transport, and engineering (Nguyen et al., 2019). Additionally, severity of consequences for CSOR typically develops in time after the DEs (e.g., containers being delayed in port due to congestion, the spread of ransomware, or fire spread from a container). These characters favor the risk concept of, $R = (DE, C, U)$ in which a risk (R) comprises a DE, its consequence (C), and their attached uncertainties (U) (Aven, 2012).

It is noteworthy here that the risk concept is different from risk parameters. Risk parameters are the derivative quantities of interest to the risk bearer to describe and differentiate one risk from another, such as the *likelihood of occurrence* (LO) and *severity of consequence* (SC) of the DEs (Vilko et al., 2019). Quantitative studies about CSOR usually use the simple definition of $R = LO \times SC$. This definition, however, does not facilitate qualitative risk description or uncertainty description of risk (Nguyen and Wang, 2018; Aven, 2012), overlooking the fact that the qualitative description of risk has been mentioned as the fundamental initial step in modern risk analysis methods (Van Der Sluijs et al., 2005; Rae et al., 2014; Bjerga et al., 2016). Additionally,

DOI: 10.29677/MR.202112_1(1).0004

while quantitative risk description provides magnitudinal and visual presentation of risk, the qualitative description of CSORs is usually limited to risk identification, obstructing a deeper understanding of the context, consequences, and risk affecting factors (Alyami et al., 2014; Chang et al., 2015; Nguyen and Wang, 2018; Nguyen et al., 2021b). This overlooking of traditional CSOR studies inhibited analytic vision into uncertainty and complexity, which has been indicated as the most prominent issue of risk analysis (Garvey et al., 2015; Renn, 2008). This unavailability of information forced prior CSOR studies to rely on experts' subjective assessments as a given indication of risk magnitude (see, for example, Yang, 2010; Alyami et al., 2014; or Chang et al., 2015).

Risk management could benefit greatly from qualitative risk descriptions. A detailed risk investigation could indicate or confirm the significance of emerging research areas where more detailed context and evidence are needed (Lee and Song, 2017). Furthermore, knowing the factors affecting the magnitudes and characters of risks is important in the qualitative risk analysis model, research design, and producing predictive risk assessments (Goerlandt and Montewka, 2015a; Goerlandt and Reniers, 2018; Nguyen et al., 2019). The extent to which a risk analysis model is progressively implemented, validated, and reliable in a real-world situation also depends on how it fits with the perspectives and interests of stakeholders in real-world situations (Aven and Heide, 2009). Therefore, the insights from interviewees in the industry are valuable as a source of data for qualitative risk analysis (Rae and Alexander, 2017).

2.2 Information operational risks (IORs) in container shipping

Operational risk has always been an active stream of research in the maritime shipping, container shipping, as well as supply chain literature, mentioned under various terms, such as disruption scenarios (Gurning and Cahoon, 2011), disruption risk (Wang et al., 2018; Ivanov et al., 2018), logistics risk, or transportation risk (Tummala and Schoenherr, 2011; Ho et al., 2015). CSOR can be understood as the potential DEs in container logistics operations that may negatively affect the supply chain members' ability to maintain their goods and services at a certain quality, quantity, and profitability (Manuj and Mentzer, 2008; Nguyen, 2020). In comparison with risk in other management levels, CSOR is characterized by higher frequency and a shorter period from the forming of direct causal factors to consequences (Nguyen et al., 2019).

The efforts of the CSOR research community are primarily on developing and applying quantitative models to prioritize risks based on quantification results of risk parameters (Yang, 2011; Chang et al., 2015). Multiple features were added into quantitative risk analyses, such as Bayesian probabilistic reasoning (Yang et al., 2008; Alyami et al., 2014), expert communication platform (Nguyen et al., 2019), and systematic uncertainty handling (Nguyen et al., 2021c). These models and their applications provide valuable insights into the overall situation of CSORs in different parts of the world. Their results, however, only provide overarching managerial implications based on the quantified magnitude of risk and uncertainty. The explanation and validation of results could benefit from a deeper understanding of the underlying phenomena of each type of DE, which requires tailored individual or categorial investigations (Lee and Song, 2017; Årstad and Aven, 2017).

Recent CSOR studies suggest a change in the relative level of risk and uncertainty in which operational risks in the information flow are gaining momentum. Although physical risks still occupy most of the highest positions, IORs are climbing up in ranking (Chang et al., 2015; Nguyen, 2020). The study of Nguyen et al. (2019) depicted IORs as a category of risk with the highest uncertainty and potential cumulative consequences.

DOI: 10.29677/MR.202112_1(1).0004

Instances of cargo misdeclaration, successful cyberattacks, and system outages have also been increasingly reported from industry, where a DE from the information flow triggers others in physical and payment flows (Tsai, 2006; Ivanov et al., 2018). The maritime shipping and supply chain industries are increasingly digitalized and automated (Fruth et al., 2017; Ivanov et al., 2018; WEF, 2020). The establishment of faster and more automated information exchange channels suggests a more connected and interdependent network, prone to domino failure effects and data ethics risks (Fruth et al., 2017; Nguyen et al., 2021a).

Cargo content misdeclaration is the main factor in catastrophic accidents related to flammable and explosive cargoes, which was observed in the case of Tianjin port (2015), Maersk Honam (2018), and various other incidents (Ellis, 2010; Loh and Thai, 2015; Cao and Lam, 2019). Failures of hardware and software components could affect the availability of the system and the integrity of the information flow (Rialland and Tjora, 2014; BIMCO, 2021). Misunderstandings or inadequate consideration of payment documents and requirements, including critical instruments such as bill of lading (B/L), exposes the shipments and the related parties to risks such as false release, commercial fraud, and multiple types of dispute (Tseng et al., 2013; Lam and Bai, 2016). Various other cybersecurity events that occurred in ICT systems of CSSPs (e.g., order/booking systems, automated terminal operation systems, ship-shore communication, ransom attacks) indicated that IORs could trigger system outages, criminal activities, and transport network disruptions (Sen, 2016; ENISA,2019).

Intuitively, one can speculate that there might be some major factors affecting the situation of CSORs, adding significance to IORs. Despite the emergence of IORs, confirmation and in-depth exploration of factors and effects influencing IORs have not been adequately carried out (Nguyen et al., 2021b). Unawareness of the complexity and uncertainty in the literature (mentioned in Section 2.1) is a significant obstacle, because CSOR assessing models cannot model the causal relationships among risks. Meanwhile, the complexity of risk networks puts a serious question on the validity of CSOR studies that rely solely on subjective assessments from experts (Rae and Alexander, 2017). An improved approach to CSOR focusing on IORs and their consequences to other flows is needed to fill this gap.

3 METHODOLOGY

3.1 Data collection

The qualitative database for this study was extracted from a larger project investigating the impact of blockchain technology on CSOR. A section of the instruments was specifically designed to gather the contexts and statuses of the industry regarding operational risks in the information flow based on a comprehensive review of CSOR literature. The prepared instruments were pre-tested and revised with feedback from researchers and Ph.D. candidates, and voluntary professionals from multiple CSSPs before being approved by the University of Tasmanian Human Research Ethics Committee. Thirty-two telephone interviews were conducted with interviewees from 19 companies. These companies include five (5) terminal operators (12 interviewees: 37.50%), six (6) shipping companies (10 interviewees: 31.25%), and eight (8) freight forwarders (10 interviewees: 31.25%) in Australia. Their position at the time of the interview and years of related experience of interviewees are provided in Table 1. The interview lengths are from 28 to 62 minutes and averaged at approximately 38 minutes.

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202112_1(1).0004

Table 1. Interviewed participants.

	Position	Exp	Code	Position	Exp	Code
Terminal operator	Terminal information manager	16	P01	Chief information officer	22	P07
	Terminal operation system manager	13	P02	Chief commercial officer	12	P08
	Technology project manager	15	P03	National landside and efficiency manager	44	P09
	National system optimization manager	10	P04	Senior operational manager	19	P10
	Chief information officer	30	P05	Chief information officer	17	P11
	Business administration manager	27	P06	Vice president of technical services	14	P12
Shipping companies	Line manager	15	S01	Digital project manager	10	S06
	Head of innovation & technology	19	S02	Blockchain specialist	15	S07
	Managing director digitalization	30	S03	Digitalization manager	14	S08
	Digital project manager	13	S04	Deputy general manager	20	S09
	eCommerce manager	15	S05	Country general manager	20	S10
Freight forwarders	State manager	30	F01	General commercial manager	30	F06
	Managing director	30	F02	National manager of intermodal	13	F07
	Global head of technology and business improvement	15	F03	Digitalization & Transformation manager	27	F08
	IT project manager	25	F04	Transition & Transformation manager	10	F09
	Digital technology manager	15	F05	eCommerce Manager	15	F10

(Exp: Years of relevant experience; Code: Interviewee's sector P: Terminal operator, S: Shipping company, F: Freight forwarder)

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202112_1(1).0004

3.2 Data analysis

3.2.1 Thematic analysis

Thematic analysis is a well-established research method for working with qualitative risk data. One of the advantages of thematic analysis is the balance between constructivism and realism (Vaismoradi et al., 2013), sometimes depicted as proceduralist (Goerlandt and Montewka, 2015b; Sørensen, 2018). Its core research activity is *thematic coding*, a process that is also employed in many other qualitative analysis methods (e.g., content analysis) (Braun and Clarke, 2006). However, thematic analysis does not pay much attention to the descriptive presentation of the dataset (e.g., frequency of code), but the interpretation of various themes emerges from the database (Vaismoradi et al., 2013). In a risk research context, the qualitative approach of thematic analysis aims at rendering risk understandings based on the perspectives of those who are bearing risk (Thomas et al., 2016).

The thematic analysis implemented in this research follows the guideline of Braun and Clarke (2006) with four main steps. First, the analyst familiarizes himself with the data through transcribing, initial reading, and re-reading transcriptions. In this study, the transcription of each interviewee was organized into a document file. All were de-identified and imported into NVivo 12, and referred to as *corpora*. Second, initial *codes* were established with collated data from different corpora, highlighting features of the database. Initiation of new codes and data collation were conducted in parallel. Third, potential themes were identified across the codes. There was an iterative process of reviewing and revising themes as codes are added in. The themes were finally defined and named based on their collated codes. Forth, results were extracted from themes with insightful discussions, backed up by compelling codes. A summary of the research methodology is illustrated in Figure 1.

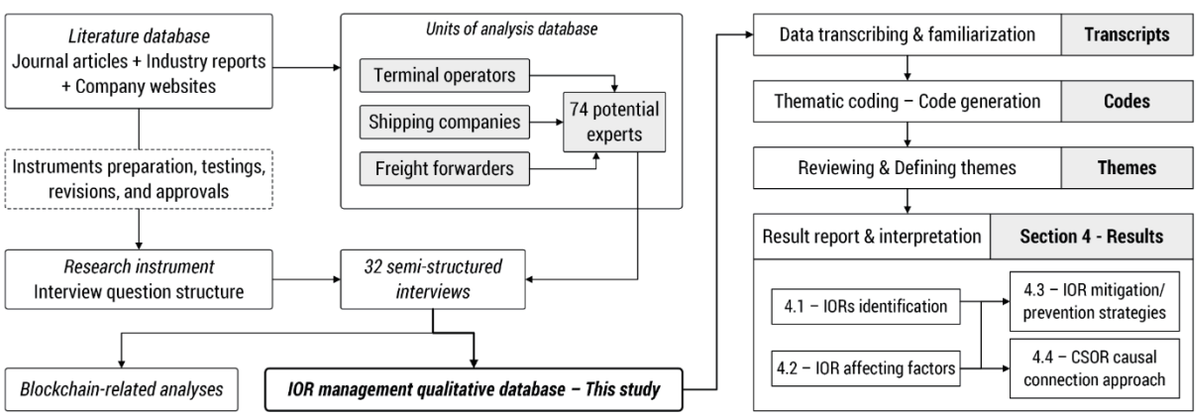

Figure 1. Research methodology and presentation of analysis results.

3.2.2 Database segregation for multiple analyses

The database for thematic analysis is taken directly from Section C of the interviews. The focus of this section is the operational Des experienced by interviewees. Since the topic is blockchain technology in container shipping operations, most of the interviewees have extended working experience with information and communications technology (ICT) systems (Table 1). Therefore, the incidents they mentioned are highly related to IORs with detailed descriptions of scenarios, responses, mitigation strategies, and risk influencing factors. Since the interviews are semi-structured, the interviewers were able to ask follow-up questions for more details after the initial questions. Table 2 describes the main objectives of questions asked in Section C and their connections to the topic of each analysis presented in this paper.

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202112_1(1).0004

Table 2. Interview questions in correspondence to topic of theme for thematic analyses.

Questions' topic	Initial questions	Topic
The interviewee's experienced DEs	If you think about the most significant events that you or your company experienced in the last 5 years, could you please describe them? What were the causes or the suspected causes of the event?	Potential IORs CSSPs' risk perception – Risk parameters
IORs' potential consequences	What were the consequences of the event?	IORs' consequences on data and information
Responses to DEs and mitigation & prevention strategies	How did you or your company immediately respond to the event? Is there any measure taken after the event to prevent or mitigate the risk?	Mitigation and prevention strategies
The significance of IORs in container shipping	Do you think that the risks in the information flow of container shipping is becoming more significant? Why do you think that?	Influencing factors of the IOR situation

4 RESULTS AND DISCUSSIONS

4.1 Identification of information operational risks in container shipping

Ten IORs with enriched details and descriptions were identified. This result suggests that qualitative data provided by interviewees are effective in risk identification and qualitative description, especially in realizing the pervasiveness of the consequences of IORs.

4.1.1 Potential DEs in the information flow

The first component in the concept of risk is the potential DEs. This section discusses the DE of each risk with references of interviewees.

IOR 1 – Human erroneous operations on systems

Human factors in information operations were emphasized by interviewees from all CSSP groups (F05-07, F09, F10, P01, P03-07, P09-12, S04, S06, S08-10). Digitalization and automation bring huge benefits for CSSPs through the reduction of headcount and enhancement of efficiency. Human capability in keeping up with this trend, however, is undermined by progressively more complicated operating systems maintained by fewer operators. This is in addition to the previous CSOR studies, in which micro-operations such as errors in planning were focused on (Papathanasiou et al., 2020). A terminal operator's CIO (P11) shared an incident: "*An employee made a mistake while operating a database application. We lost system availability as well as the data. Even with our internal team, external experts, and vendor support, in the end, it still was not successful.*" With shipping companies, the flow of information is not only onshore; there are also connections to the fleet operating in the high sea. Managing information onboard the ships and the connection between onshore and offshore systems is critical for agile and safe fleet operations.

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202112_1(1).0004

IOR 2 – Failures of software components

Modern container shipping requires a range of software components to operate (ENISA, 2019). For example, terminal operating system (TOS) are typically connected to other systems such as enterprise resource planning (ERP), optical character recognition (OCR), or radio frequency identification (RFID) systems to enable real-time monitoring and decision-making (Heilig and Voss, 2018). All CSSP groups mentioned this risk (P03, P05, P09, P11, S08, F03). The software components can contain (1) software bugs (i.e., programming faults) or (2) errors stemming from discrepancies between the simulated environment (e.g., software architecture and programming) and the real-world situation. For example, a national landside and efficiency manager (P09) experienced several situations in which a newly implemented automated TOS failed to meet the expected performance because it was developed in-house and then implemented in different terminals without adjusting to each terminal's characteristics (e.g., yard size). Fierce competition and unfavorable market conditions forced many CSSPs to focus on their core value and outsource certain software components and solutions (Shi and Chan, 2010). This dependence also introduces risks of software failure and third-party dependency on the system.

IOR 3 – Cybersecurity breaches and attacks

The concern over cybersecurity risks is well-observed across different CSSPs with a high frequency of codes. Twenty-three (23) out of 32 interviewees (~72%) mentioned it as a significant IOR (F01, F02, F04, F05, F09, F10, P01-06, P08, P09, P11, P12, S02-05, S07, S08, S10). This concern is in line with other reports from the industry (Sen, 2016; Global Maritime Issues Monitor, 2018; Johnson, 2018) and previous CSOR studies (Nguyen et al., 2019; Vilko et al., 2019). Interviewees consider the Maersk cyberattack in 2017 as an eye-opener for the industry about the potential of a cybersecurity breach. In this attack, the perpetrator hijacked an update server of a government agency. All companies who established a communication channel received updates from the server, bringing the malware into the company's network. A detail that may have been overlooked in previous studies is that a cybersecurity breach does not have to be entirely in cyberspace, meaning that cybersecurity has to be considered together with physical security to prevent coordinated unauthorized access. A deputy manager (S09) recalled an incident: "*They had a break-in in their office, but they did not notice. It was a fake cleaning group placed USB sticks in all the computers to extract and send data*". Additionally, threat actors might use multiple techniques to investigate or establish inside connections to facilitate the breach. This poses a safety risk for employees who have significant information access or critical system knowledge.

IOR 4 – Incompatible data exchange processes

Differences regarding the channels and standard format of data exchange may undermine the performance and integrity of the information. Interviewees mentioned communication failures and inefficiencies caused by differences between CSSPs and their partners regarding the channels and standard data exchange format (F07, F09, S05, P03). This is a chronic IOR in the container shipping industry and along the supply chain (Chang et al., 2015; Nguyen, 2020; Carlan et al., 2020). Due to the nature of the business, freight forwarders seem to be exposed to this risk more than other CSSPs with clusters of systems that handle various sources and formats of information. This DE can also obstruct the development and implementation of innovative solutions, mainly due to poor data and communication quality. A transition and transformation manager (F09) reflected that while intending to apply technologies for a better-featured information flow, the infrastructure is not adequate for implementation. In severe cases, even bidirectional data exchange cannot be guaranteed.

DOI: 10.29677/MR.202112_1(1).0004

IOR 5 – System outage

This is a widely mentioned risk by CSSPs (F03, F04, F06, F09, F10, P01, P04, P05, P09, P11, P12, S04, S05, S08). Unavailability of systems heavily affect, or in some cases eliminate, the capability of CSSPs in monitoring, controlling, and carrying out crucial container shipping operations. The outages of systems also impact related systems of partners that rely on it as a source of information. For example, a global head of technology and business improvement (F03) described an outage of a data exchange platform:

> *"The situation went on for half a week. And that means all normal digital transaction processes had to be handled manually. Our colleagues have to enter the booking request, shipping instructions, B/L information into our backend system that caused a huge amount of extra manual works."*

Meanwhile, the sensitiveness of terminal operators toward system outages stems from the fact that their competitive advantages are based on price, handling time, and productivity (Lee and Song, 2017). System outages can cause more operational and financial impacts to automated container terminals, where container handling operations rely on a constant stream of information from a vast array of IoT devices and multiple support systems for situation awareness and control (Sen, 2016; Heilig and Voss, 2018). The recovery process for those terminals is especially time- and effort-consuming, since each component of a complex cyber-physical system must be recovered consecutively. A significant concern has been expressed concerning centralized platforms that collect, process, and distribute information and data along the container supply chain. A national system optimization manager of an international terminal operator (P04) even speculated: "*If they were impacted or got under an attack, that would be chaos. We are now fully relied on those systems. If they stop working tomorrow, terminals will take even weeks before they can do anything*." System outages can be triggered as a response to a large, imminent threat. This sacrifice is an effort to circumscribe the potential consequence until the threat is identified and eliminated.

IOR 6 – Failures of infrastructure or hardware components

The operations of IT systems require continuous supplies, such as power and internet connectivity. Interviewees mentioned multiple incidents of infrastructural failure (F03, F04, F09, P01, P04, P05, P07, P09, P12, S04, S08). For example, the recent Australian bush fire caused incidents of losing communication and power in container terminals. Other incidents such as broken internet cable due to construction operations and power supply unit malfunctions were also mentioned. These incidents can affect both the availability of the systems and the integrity of data stored, even with redundancy and backup systems. A digital project manager (S04) described the situation in his company: "*Every time there is a disruption to our mainframe server in the US, there is basically a global business disruption for our system. If the supply unit is out, then no matter how much redundancy you prepared, the outage still affects the whole system*".

IOR 7 – Ransom acts

The recent studies suggest an increasing trend of malware penetrations of CSSPs' IT systems (Global Maritime Issues Monitor, 2018; ENISA, 2019), causing damages to data integrity, operation continuity, and the systems themselves. Well-known cases of cyber-ransom were taken as examples by many interviewees (F01, F02, F03, F09, F10, P02, P05, S02, S10). Once a key system is gained control of or crucial data is taken hostage (e.g., customer or employee personal data, pricing data, digital assets), the threat actors could demand ransom for the release of hostages, further impacting the victim. For example, a recent cyberattack on a freight forwarder was highlighted by freight forwarder interviewees F10 and F03 in which the hackers demanded ransom with the threat of releasing leaked data into the dark web. The case was considered critical for the company because it lost control of its customer data, risking its reputation, business, and lawsuits related to data and privacy protection.

DOI: 10.29677/MR.202112_1(1).0004

IOR 8 – Unexpected changes, requirements, and postponements of documents/formalities

Although this risk has been mentioned in previous CSOR studies in the form of delays due to uncertainties of paperwork for the container to import/export (e.g., custom clearance, biosecurity clearance) (Chang et al., 2015; Nguyen and Wang, 2018), the recent restrictions and changes of policies due to COVID-19 have increased this risk with cases of severe delay, container abandonment, and port congestion (F01, F02, F06, P02). The impacts come from the immediate changes of export/import policies and the resonant effects from lockdown policies along the supply chain. For example, a freight forwarder managing director (F02) described the situation of his customers:

> *"They have put all their volumes into the cheaper suppliers in China. There are up to 160 days until their products can be shipped. And literally, they cannot get reliable delivery. The normal schedule of shipping lines has been blocked or cancelled. And this makes predicting when goods can arrive a million times more difficult."*

IOR 9 – Inaccurate information input/submission

Cargo misdeclaration has been highlighted as one of the most frequent IORs that might result in catastrophic events (Chang et al., 2015; Nguyen, 2020). Maritime accidents caused by misdeclaration of cargo type and weight can also inflict casualties (F10, P01, S04, S10). Alarmingly, the list of events continue to lengthen even with prevention measures (e.g., random inspection, verified gross mass requirement) and advanced technology solutions in place. Nevertheless, it is still dependent on the shipper's knowledge and his representatives to pack, load, and declare the cargoes truthfully and correctly. Without this knowledge, it is difficult for the CSSPs to implement proper safety procedures. Interviewees from all three groups of CSSPs agreed that better data quality should be prioritized, even with the promising advent of technologies. For example, AI technology can confidently identify whether shipments are suspicious and recommend pre-loading inspection, though it requires good quality data to be reliable.

IOR 10 – Information asymmetry/incompleteness

The flow of data in the container shipping industry contains sensitive information, such as pricing structure. Different from terminal operators, shipping companies and freight forwarders are more susceptible to this risk (F02, F03, F05, P03, S04, S07, S08, S09, S10). This type of DE can be triggered by the leakage of information resulting from other IORs. A shipping company's digitalization manager (S08) explained the prudent approach of carriers in sharing information, even though they are long-time partners or operate in the same alliance:

> *"We also operate on the vessels of our competitors. We need each other's data, but nobody likes to share data. In our industry, prices are not public. The structure of prices is very complex. A lot of customers will try to find out this information and then try to sell them to somebody else."*

4.1.2 Potential consequences of IORs

The causal relationships between IORs and operational risks in physical and payment flows can be realized by looking at the DEs' immediate consequences to data and information. Qualitative analysis can provide a more detailed description of triggering connections between CSORs. In this study, four categories of consequence were identified as the gateways from IORs to risks in other flows, including delay and unavailability, loss and corruption, leakage and theft, and inaccuracy and manipulation.

DOI: 10.29677/MR.202112_1(1).0004

Consequence 1 – Delay and unavailability of data

Delay and unavailability of data directly affect the timeliness and synchronization between operations of CSSPs. The most apparent consequences are delays in transportation (e.g., rollovers, port skips) and congestion at container terminals. Moreover, this consequence obstructs the efforts of parties along the container supply chain in logistics management. Unavailability of track-and-trace information directly causes poor visibility over the supply chain, which has been discussed extensively in supply chain management literature as the trigger of demand and inventory risks (Tummala and Schoenherr, 2011; Ho et al., 2015). Although maritime shipping is more resilient toward delays, delays of perishable goods still pose risk of cargo degradation (Nguyen et al., 2019). Additionally, unexpected delays or changes of documents/formalities can lead to container abandonment, an issue with both shipping companies and terminal operators. There are also cases of data unavailability resulting from the fear of information asymmetry/incompleteness that affect the feasibility of innovative and feature-filled digital solutions. For example, a shipping company's digitalization manager (S08) recalled project desertion due to a data-sharing disagreement between shipping companies in the same alliance: "*We had a very good idea many years ago to visualize on a map the position of the container. But we could not agree with our partners to show their vessels on our system.*"

Consequence 2 – Loss and corruption of data

The extent of consequence caused by losses and corruption of information depends on the type of data and the systems and data recoverability. If the data lost are not recoverable, they must be regenerated or inputted to be available again, exacerbating the consequences in the physical and payment flows. The availability of data backups is the keystone of Maersk's NotPetya recovery (Greenberg, 2018). In Maersk's 2017 attack, the Windows systems were eliminated, leaving the company with no visibility of the core systems. However, because the key capacities of the company were powered by other operating systems (e.g., Linux), even though the Windows shell for monitoring was not available, the core systems for operations behind that were not significantly damaged.

Consequence 3 – Data leakage and theft

Interviewees describe this consequence as more frequent than the unavailability or loss of data as the result of cybersecurity breaches in the container shipping industry. Interviewees from terminal operators and freight forwarders indicated a critical consequence of data leakage in which container loss is caused by leakage of shipment's content and incorrect cargo release. This risk is observable through real-world incidents at container terminals where a malicious actor has obtained a PIN code to release the containers. A terminal operator's technology project manager (P03) mentioned:

> *"The problem of PIN numbers are happening right now with many ports since this critical information is just flicked around in emails. If somehow you send the email to the wrong person or someone has it and want to pick up the container that they do not own, they can do it."*

Apart from causing information asymmetry/incompleteness and potential loss of volume and customers, leakage and theft of data, especially customer data on a large scale, can also severely affect the victims' reputation through two causal mechanisms: (1) being seen as neglected or incompetent in securing data and (2) cybersecurity breaches of CSSPs might result in service disruption, affect their capability in maintaining services (see IORs 3 and 5). Additionally, the victim may face investigations and fines from regulatory bodies based on data and privacy protection laws. Data leakage is also a factor in other criminal activities such as drug and human trafficking using containers.

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202112_1(1).0004

Consequence 4 – Inaccuracy and manipulation of data

The typical prior DE of Consequence 4 is cargo misdeclaration, which originates from two primary causes. First, the willingness and capability of the customers to understand their cargoes' natures, packing protocols, and declaration processes might be limited. Second, financial benefits might encourage cargo misdeclaration. Shippers can avoid additional surcharges or procedures by wrongly declaring a potentially dangerous shipment or putting in an incorrect container weight. There are also other cases, such as outdated or incorrectly informed certificates of seaman or vessels. The consequences of inaccurate data can easily spread to physical and payment flows. As CSSPs cannot obtain complete or truthful information, safety protocols (e.g., safely handling, position planning) cannot be deployed, leading to catastrophic events with dangerous cargo. In less-severe cases, cargoes and vessels may be detained, causing further shipping delays. Towards terminal operators, manipulation of information regarding container movement and release might lead to loss of containers and underground activities such as drug trafficking.

4.2 Influencing factors of the IOR situation

Most of the interviewees (~85%) agree that the operational risk in the information flow is becoming more significant than before. Based on the reasoning of interviewees, this study identified six main factors adding gravity to the situation of IORs.

Factor 1 – Complexity and ambiguity of the information flow

There are different types of data with different extents of importance and required speeds of transfer in container shipping flow of information. A shipment can involve numerous parties with various schemes and settings of the dataset, from simple emails to EDI transmission. The flow is fragmented and mainly established and maintained bilaterally between parties. CSSPs, especially freight forwarders, have to develop a managing system that contains different components to handle such a flow of information. A national intermodal manager (F07) described his company complicated IT infrastructure: "*We have to pay a lot of money to establish and maintain our fragmented systems, which are carefully designed and every part of it needs years of developments, trials, and modification*". This complexity amplification is an immediate result of inefficiency and insecurity of the overall cyber-physical system (Zio, 2018). Additionally, through time, isolated data exchange channels develop their own customizations, such as taxonomy and data format, aggravating the fragmentation. The complexity of these cyber-physical systems complicates the efforts of CSSPs to be adequately aware of IORs.

Factor 2 – Increasing dependence on fast digitalization and automation

With the potential optimization through real-time information exchange and reduction of headcount, many parts of the container shipping supply chain now depend heavily on data availability for automated processes (e.g., automated terminals and warehouses, EDI exchange, electronic container release). Information DEs, therefore, can easily trigger the same DEs in other connected systems and other DEs in the physical and payment flows, causing pervasive consequences. Meanwhile, IT systems are developed and implemented quickly to achieve a competitive advantage, making them prone to bugs and vulnerabilities. S04 shared his experience in developing digital solutions for a shipping company:

> *"We discovered that if you are now spending two years with a project, by the time that you go live, the project has already been outdated. You need to move quicker, but that means there are mistakes, in the IT backbone, or the processing, even sometimes in the foreground on the website or the portal."*

DOI: 10.29677/MR.202112_1(1).0004

These digitalized and automated systems are also more vulnerable and take longer to recover after a DE. A CIO (P05) described a case of terminal shut down by a cyberattack in which the recovery is significantly more time- and effort-consuming compared to other terminals. In addition, it is impossible to recover a long list of interdependent and interconnected systems immediately.

Factor 3 – Inadequate IT infrastructure of the industry

While advanced technologies like AI or blockchain are beginning to be adopted, many parts of container shipping's information flow are still obsolete. This environment is favorable for IORs and obstructs the implementation of new solutions. Outdated legacy systems manage many processes. A global head of technology and business improvement (F03) shared that his company operates over 500 systems with a large proportion that is out of date. They need regular maintenance, and their failures are often followed by the outage of others, including some key operational systems. The lack of trust and underdeveloped information flow prevent a smooth flow of communication between CSSPs. For example, the structure of alliances between shipping lines is more about shipping network optimization and less about building a rich information exchange channel (see Consequence 1). Considering current cybersecurity threats, which are extremely well-funded and well-prepared, it is not a sustainable situation.

Regarding data exchange protocol, even though several CSSPs are moving to application programming interface (API), most of the exchanges still use EDI, which has been used for decades. It is not only interpreted and implemented differently by CSSPs, but also reported as poorly scalable. EDI's limited ability to keep up with real-time information exchange puts increasing pressure on CSSPs, since the supply chain managers and users demand better data for better controllability, lower costs, and faster adaptive decision-making (e.g., coordination of sea-land at port, inventory management).

Factor 4 – Stakeholders might not fully realize the significance of IORs

In a competitive market, it might be difficult for CSSPs to invest a significant proportion of their budget for IT development and cybersecurity, especially when returns are difficult to realize in the short-term and uncertain. Several interviewees at terminal operators and freight forwarders mentioned that despite the importance of IT and IT knowledge management in CSSPs, their available budget for IT improvement and transformation is overstretched. A TOS manager (P02) shared his difficulty in having adequate attention of the executive board toward IORs, even after catastrophic examples in the industry: "*If I want to convince the top management for IT investment, I will have to bring them true stories with concrete evidence that help them feel the threat*". In some extreme cases, even the most senior IT overseers cannot adequately comprehend the extent of risk they are facing (Greenberg 2018).

Factor 5 – Human operators become the weak and vulnerable link in the system

The capability of the operators, supervisors, and managers in operating and maintaining the availability of the IT systems is crucial (IOR 1). Progressively more stable, secure, and automated information processes encourage the threat actors to focus on human operators as the weakest links. Social engineering and personal attacks have become a more popular and effective attacking technique than breaking battle-hardened security protocols (Sen, 2016; ENISA, 2019). Interviewees in this study confirmed this trend with incidents of bribing and threatening for information. Additionally, the skill sets of human resources in the preparation and execution of contingency plans and response to unprecedented events are mentioned by multiple interviewees as a potential disruption in the risk managing capability of their companies. A senior manager with more than 40 years of experience (P09) shared his experience with the new generation of operators and managers in system outages:

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202112_1(1).0004

"Half of the staff do not know how to do it (specific operations) manually or have never been exposed to such operations. They have the degree, but they still have not experienced a lot of disruptions… One of the most important things in designing a contingency plan is that you have the people being aware of how things work. But people begin to think all you have to do is press the button."

Factor 6 – Cybersecurity is a substantial IOR

There are four qualities of data and information from the viewpoint of CSSPs, including availability, timeliness, accuracy, and privacy (see 4.1.2), which cybersecurity breaches can threaten. The container shipping industry is relatively inexperienced regarding cybersecurity. Interviewees mentioned three main subfactors.

First, threat actors are becoming more sophisticated, knowledgeable, and coordinated. Multiple vectors are now used by attackers, from well-known social engineering techniques like phishing emails to coordinated DDoS and malware attacks (Bissell et al., 2020). For example, an experienced CIO (P05) recalled a cybersecurity breach where the perpetrator posed as an electrical contractor. They placed data loggers in power strips, which were later collected, and then keystrokes were analyzed for information and passwords. Second, the motivation of cybersecurity breaches is not simply financial. CSSPs now have to deal with threat actors that are better prepared, on a larger scale and even state-aided. Although being rare, catastrophic cybersecurity incidents can stem from geopolitical instabilities, such as Russia – Ukraine, USA – China, Australia – China. In such attacks, transportation infrastructures are likely the target, and in most cases, the truth about the perpetrator might never be revealed or declared. S02 mentioned an experience in which his company was caught in a state conflict: "*We think 100% confirmation may never be discovered. This attack looks like a ransomware, but that was just a façade, the actual purpose of this malware is pure and only destruction. We were just collateral damage*". Third, internal factors are easy to be overlooked and ignored. An overused assumption is that the threats come from outside of the organization, which is usually not the case with many incidents in the container shipping industry. In line with Factor 5, several IT managing interviewees in this study still considered personal manipulation, bribing and threatening individual employees the strategy of choice for the threat actors.

However, as Factor 4 suggests, the stakeholders and decision-makers might not be aware of those subfactors. These results suggest more eye-opening incidents in the near future if there is no improvement or only superficial improvement from the CSSPs to stay ahead of the game against cybersecurity threats.

4.3 Mitigation and prevention strategies

Six primary strategies were recommended in this study. The strategies reflected risk analysis followed by well-designed and multipronged mitigation/prevention plans being the key to protecting and improving the information flow. It is noteworthy that citations to supporting previous studies will be made in the discussions of the strategies to improve the credibility of arguments and the strategies' persuasiveness.

Strategy 1 – Conduct risk analysis as the basis for mitigation and prevention

This strategy was mentioned by multiple interviewees (F01, F10, P02-04, P09, S03-05). CSOR managing activities are often organized based on a pre-allocated budget (ENISA, 2019; Bissell et al., 2020), the relative magnitude of risks, and the details of potential DEs (e.g., scenarios of failures and solutions) (Johnson, 2018; Bissell et al., 2020). The resilience and contingency plans should be designed in proportion with the magnitude of risks. A TOS manager (P02) emphasized that risk management is organized depending on the budget provided, which requires a risk analysis to assess the probability and potential consequences of a large range of events. Such assessments can only be obtained reliably through a thorough quantitative and qualitative risk analysis. An important component of the analysis of IORs is to evaluate the current capability of the whole system in the conjectured Des. Internal and multilateral drills and mock tests help prevent risk complacency and make the stakeholders aware of the actual risk and effectiveness of implemented measures (S02, S04) (Årstad and Aven, 2017).

DOI: 10.29677/MR.202112_1(1).0004

Strategy 2 – Develop a professional and transparent culture toward IORs

This strategy was recommended by interviewees from all CSSP groups (F01, F04, F05, F08, P05, P12, S03, S08). A common agreement among interviewees is that the overall reputational impact of IORs is not yet extreme at the moment, especially with information delay or leakage. Customers and partners of CSSPs can tolerate a certain level of operational impact on their system. For example, a managing director digitalization (S03) explained that a delay of several hours up to a day might be considered medium to high operational impact with terminal operators, but only minimal to none with the freight forwarders or consignees. However, larger events such as system outages for several weeks and customer information leakage on a large scale, or repetitive events with significant consequences might eventually have a significant detrimental effect on the CSSPs' business. With those cases, the company's honesty and manner of response directly affect the reputational impacts of events. Maintaining a continuous channel of communication with other parties to provide them with updated information of the DEs, suggesting alternative logistics solutions and even timely financial compensations, proved to be effective in protecting the brand image against reputational damage. A terminal operator's CIO (P05) commented on two cases of his company's partners, here represented with X and Y:

> *"X did an extremely good job of being professional, honest, and transparent about what had happened, of being engaged with customer and public. I think its reputation actually grew stronger after the incident. Compare that to Y, they were hit with a ransomware attack, and for at least seven days, they positioned that as the extended maintenance of their system. They were then attacked again but still did not immediately confirm it."*

Strategy 3 – Prioritize the development of contingency plans and cybersecurity education

It has been shown that companies with better cybersecurity do perform better against breaches (Bissell et al., 2020). A general commercial manager (F06) explained that cyber insurance packages could not fully cover IORs in aspects such as reputational damages, loss of customers, and expected revenue. The capability of the company itself in preventing information DEs is, therefore, important in risk management. In this aspect, training and education of well-designed policies throughout the organization are critical to IOR prevention (F01, F05, F10, S02-04, S06, S08, S10). In DEs, speed of reaction and containment decisively affect the severity of the consequences (e.g., local system shutdown to circumscribe a ransomware attack) (F01, F04, F06, F09, P05, P12, S02-04, S08). An important component of IOR resilience is the readiness and deployment speed of business continuity plans. To ensure the reliability and effectiveness of those plans, redundancy in the system and network design (e.g., backup servers, multiple CSSP partners) is crucial. Therefore, monitoring and detecting DEs across systems is a key to IOR management (F01, F02, P02-05, P08, P09-12, S03-05, S08). Plans and policies need to be continuously reviewed and revised to keep up with the dynamic risk situation (e.g., business continuity plans, preventive policies). Regarding this aspect, the container shipping industry, especially larger companies with a larger budget, seems to learn and react quickly after major IT incidents. Multiple interviewees from all three groups of CSSPs mentioned that their companies conducted analyses and collaborative investigations with partners after the Maersk 2017 incident to upgrade the data exchange channels to the security standards (F01, F05, F06, F09, F10, P03, P06-09, P12, S04, S05, S08). The increase of invest ments in revamping their own systems and new R&D pilot projects in IT is showing the adoption of this strategy.

DOI: 10.29677/MR.202112_1(1).0004

Strategy 4 – Transform the IT infrastructure by better system design

Multiple IT managing interviewees mentioned redesigning their systems with a different philosophy for better security, convenience, and stability after the rise of modern cybersecurity issues (F01, F06, F09, F10, P03, P05, P09, S02-05, S08). Following this strategy, companies choose technologies as a line of defence and comprehensively designs processes with checkpoints and balanced controls to improve resilience. The most frequently mentioned strategy is the isolation and localization of multiple sectors for different functions with higher degrees of real-time system monitoring. Core systems, such as TOS, should be more isolated and protected to prevent and mitigate data loss and corruption (see Consequence 2) (F01, F06, P06, S02, S08). A head of innovation and technology (S02) explained the rejuvenation of system design after a catastrophic event:

> *"Back then, we still had a very traditional security setup that focuses on keeping the threat outside. But the moment you infiltrate, you can go everywhere. We now have created a much more contained and localized setup where individual areas and PCs can be filtered out if something suspicious happened without having to take down the entire network."*

Strategy 5 – Improve interoperability for sustainable IT development

Interoperability is an underdeveloped area in container shipping (See Factor 3). This strategy was recommended by F03, F09, P02-05, P07, P09, P11, S04, S05, S08, and S10. All interviewees in this study consider standardization across related parties, including terminological (e.g., the definition of business terms) and technical (e.g., API framework) to be an urgent objective for sustainable digitalization. Fragmented and bilaterally maintained communication channels make centralized solutions (i.e., a platform or software) more attractive to all parties in the chain since they do not have to deal with many channels separately. However, this situation creates single points of failure that can compromise multiple supply chains in the case of DEs. Standardization is, therefore, the key element for multilateral communication and sustainable IT development. Therefore, the role of associations in building, promoting, and pushing standardization forward is much clearer (WEF, 2020).

Strategy 6 – Actively involved in shaping up new information technologies

Different technologies are being implemented by big CSSPs to increase digital capacity and system optimization and risk mitigation and prevention (F07, F09, F10, P07, S02, S04-06, S08). Cloud computing was successfully integrated into the ICT systems of CSSPs to migrate cybersecurity risks and reduce other IORs. A digital project manager (S06) disclosed his company's evolution to cloud services: "*We are now migrating to a cloud platform because it is much easier to share data. We are also moving to API from EDI, which is much easier and faster if your system is in the cloud*". The involvement of technology giants such as IBM, Oracle, and Ant Group, with the biggest container shipping companies in the industry in establishing blockchain initiatives to renovate the flow of information, suggests the potential effectiveness of Strategies 4 and 5 (WEF, 2020; Carlan et al., 2020). Additionally, meaningful and rational implementations of innovative solutions can be a competitive advantage of the pioneers against the followers in innovative technology implementation. A platform like TradeLens can leverage AI and Bigdata for various other applications built on top of a good quality database.

DOI: 10.29677/MR.202112_1(1).0004

4.4 A complementary approach toward CSOR analysis

The confirmation and detailed descriptions of both risks and their potential consequences suggest a complicated risk situation with the causal connections from IORs to other CSORs. Therefore, the traditional approach of relying on risk parameter assessments to quantify CSORs (see Section 2) has become less reliable as a method of risk prioritization (Rae and Alexander, 2017; Fang et al., 2012). This paper proposes a complementary approach for risk assessment in which risks are quantified based on two methods. The first method assesses risk individually using the traditional approach. For that, Section 4.4.1 establishes a risk parameter structure based on CSSPs' description of experienced DEs. Then, section 4.4.2 proposes the framework for an additional method of choice, focusing on taking the causal connections into account.

4.4.1 Gauging risk magnitude – Risk parameters

A majority of recent CSOR studies used the parameters suggested by FMEA (Alyami et al., 2014; Nguyen et al., 2019). This structure, however, contains parameters that have strong causal connections and are difficult to validate. For example, the parameter of Detectability proposed by Nguyen and Wang (2018) consists of *Possibility of risk being undetected and Detection lateness*. This analysis shows that these two parameters determine the *Likelihood* and *Severity* of the DEs, respectively, suggesting a strong correlation between them. For example, a digital transformation manager (F09) described the triggered system lockdown of a freight forwarder in a cyberattack to stop potential malware spread (lowering likelihood) and change to manual data handling (lowering consequence):

> *"Suddenly we have to be very careful and think about what measure do we have to take. Most of the system integrations between a carrier and a freight forwarder are fully automated. So now, you have to stop that automation, close everything down and break the link to avoid the spread of the malware. And at the same time, you have to do things manually on both sides."*

With such a potential of correlation, they should not be considered separate and reliable parameters, especially for professionals from the industry to assess risk. On the other hand, the specification of severity of consequence to the three aspects of *operational*, *financial*, and *reputational* was used by interviewees in describing their experience with DEs in the information flow. The operational impact was mentioned as the disruption to the normal day-to-day functionality and continuity of the CSSPs (e.g., human resource dispatch, ongoing development project suspension, rescheduling operating plans, reallocation of resources). Additional expenses (e.g., costs, fees, surcharges, fines, compensations) and expected revenue losses directly resulting from a DE were described as the financial impact and do not include finances for risk mitigation and prevention measures. Reputational impact damages the brand image of the CSSPs and can result in complaints, decreased volume, or even loss of the whole business agreement. For example, an IT managing interviewee (F03) described the consequence of a recent cyberattack:

> *"Every day we are not able to take bookings, we lose revenue. Most of our key systems were offline for over a week. That is a significant amount of revenue. We have to spend money for external parties to help us get back online and divert our resources to manual operations. However, there is also reputational damage because we were not able to meet our contracted service level agreement. We also cannot be as responsive to our customers, and they lose trust in our security and the safety of their information with us. In some cases, we have lost business. We are potentially at risk of fines from regulatory bodies based on, for example, GDPR."*

Marine Research of the National Academy of Marine Research
DOI: 10.29677/MR.202112_1(1).0004

A risk parameter structure, as in Figure 2, is recommended from the viewpoint of CSSPs. It is built based on interviewees' default perspective of risk, and is thus suitable for the use of interviewees' cognitive capability to formulate CSOR subjective or intersubjective assessments, following the *domain knowledge and private information* expertise mechanisms (Rae and Alexander, 2017; Nguyen, 2020). This structure shows that professionals' building of risk's magnitude is relatively simple, suggesting against the use of over-complicated parameter sets with expert subjective assessments.

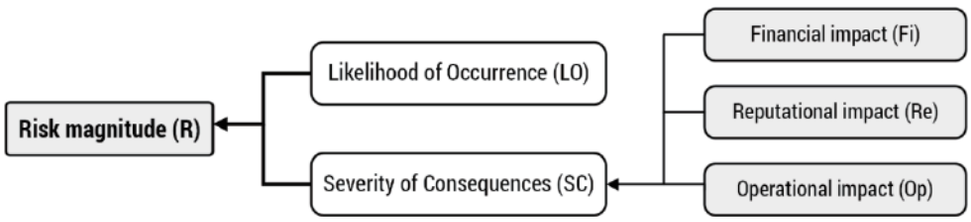

Figure 2. A risk parameter structure for CSOR assessment.

4.4.2 Risk causal connections and risk network analysis

A well-known issue with CSOR analyses is their lack of considering multiple-event risk scenarios, which has become a significant knowledge gap in addressing IORs (See Section 2). Without a more insightful view into the connections between DEs within the information flow and other flows, it is difficult to fully rely on experts' subjective elicitations of probabilities and degrees of belief for risk mitigation/prevention and strategic decision-making. Furthermore, the high connectivity between risks requires additional components to the existing risk analysis models. Based on the understandings derived from thematic analysis, this study proposes an approach to analyze CSORs considering the gaining criticality of IORs (Figure 3).

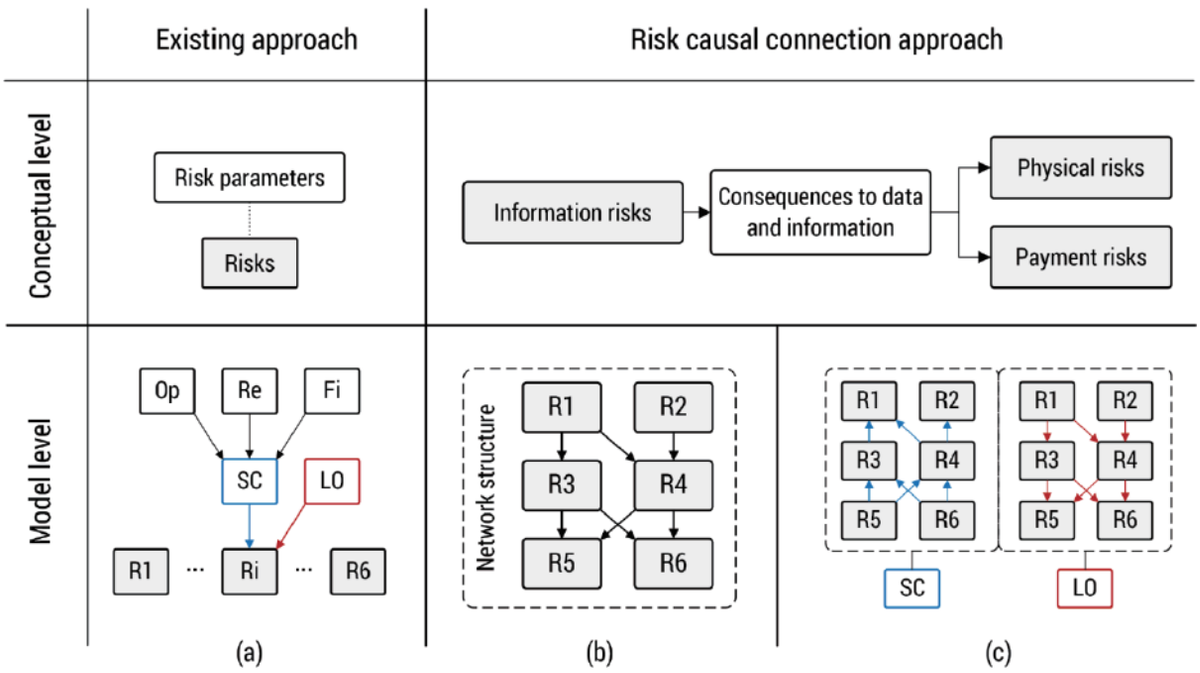

Figure 3. Risk causal connection as an additional approach to CSOR.

DOI: 10.29677/MR.202112_1(1).0004

In this approach, apart from the traditional assessment of individual risk (i.e., single-event risk scenarios), the risk analysis also includes a module of identifying the causal connections between these risks. For example, a cyberattack can result in leakage of data related to the freight structure of the company, which might trigger effects of information asymmetry and cause a decrease in shipping volume. With such a map of causal connections between risks (risk network) (Figure 3b), an overview of the pervasive effect from the information flow to other flows can be realized. Network analysis techniques are helpful here to quantify the importance of the connections (e.g., edge centrality) and individual risks (e.g., node centrality) (Fang et al., 2012).

A deeper analysis level can be enabled by quantifying the strength of the causal connections (e.g., the probability of a DE triggering another DE). Quantified properties of edges enable the propagation of different node properties across the whole risk network. For example, Figure 3c illustrates the propagation of likelihood and consequence severity using the network structure in Figure 3b. Those propagated results can then be compared to the direct individual assessment results (Figure 3a) in an uncertainty analysis. Here, the analysis will provide insights into the epistemic status of the risk situation, both in the sense of predicting future events (outcome uncertainty) and incomplete knowledge base to do so (evidential uncertainty) (Nguyen et al., 2021c). Additionally, the risk analyst can analyze the most likely and/or devastating multiple-event risk scenarios. Multiple tools are available for this task, such as Bayesian Network, Evidential Reasoning, Monte Carlo simulation, and Network Entropy. Establishing different checkpoints for the triangulation of results is critical to validate the analysis. This cannot be carried out through reality checks for large cyber-physical systems in container shipping or maritime logistics (Aven and Heide, 2009; Goerlandt et al., 2017).

This approach is fundamentally different from the existing approaches because it does not aim to predict the "true" pre-determined value of risk. Instead, it recognizes the uncertain and dynamic nature of risk. It focuses on describing the situation of CSOR more explicitly with more available information regarding its complexity and uncertainty. For example, the network analysis could be deployed to identify the important risks or connections considering the multiple-event risk scenarios. This method provides valuable insights into optimizing risk prevention efforts (Nguyen et al., 2021a; Fang et al., 2012). Hence, the experts' influence could be reduced to less ambiguous and straightforward tasks, such as assessing the potential likelihood of the causal connection.

DOI: 10.29677/MR.202112_1(1).0004

5 CONCLUSIONS

Evidence from the CSOR literature and observed DEs indicates the increasing significance of operational risks in the information flow. However, multiple fundamental elements for quantitative IOR analysis are missing, obstructing an in-depth understanding of the subjects of interest (e.g., risk prioritization, uncertainty analysis). This study utilized thematic analysis to dig deep into the qualitative database collected from 32 interviewees of 19 CSSPs, including terminal operators, shipping companies, and freight forwarders. The analysis provided fundamental understandings toward IOR DEs, their consequences, affecting factors, and mitigation/prevention strategies. A CSOR approach is suggested based on those analysis results, focusing on using network models to capture causal connections between CSORs.

For the CSOR and maritime logistics literature, this study highlighted the role of qualitative analysis in risk description, particularly in risk identification, consequence realization, and triggering connections between DEs. The results show direct connections between DEs in the information flow with consequences to the avail ability, timeliness, accuracy, and privacy of data, and ultimately, the physical and payment flows. IORs were described with a rich qualitative database, revealing multiple aspects out of the reach of quantitative analyses. This paper also suggested a structure of risk parameters suitable for qualitative analysis, including the likelihood of occurrence and financial, reputational, and operational impacts of the DEs. A complementary approach in quantitative risk analysis was proposed to tackle the potential complexity and uncertainty of IORs. The approach relies on modelling the risk situation by a risk network, allowing an additional assessment that takes causal connections between risks into account.

To the container shipping industry, this study underlined the rise of IORs as the inevitable side effect of fast and unsustainable digitalization. The contingency plans have to be ready and continuously evolved with the situation of risks, but speed and manner of response to DEs also directly affect the consequential impacts. While interoperability and new technologies are key strategies against IORs, they are hampered by a lack of fundamental elements such as industry standards, the vision of decision-makers, and trust between CSSPs. This issue resulted in the industry's moving toward complex, fragmented, and bilateral information channels between parties in the supply chain and centralized points of failure. In addition, the underdevelopment of the container shipping industry's IT landscape and a "digital gap" of human resources create opportunities for cybersecurity breaches, which has become a huge issue in recent years.

A range of research directions is suggested from these implications. First, the quantification of identified IORs using the recommended set of parameters will help describe the risk situation with more concrete evidence in a more specific setting (e.g., a company, a country, a region). Second, the high connectivity of IORs can be modeled by a network of nodes from DEs in the information flow to other flows, allowing systematic analysis of multiple-event scenarios. Third, IORs may be investigated individually to understand better risk at a micro level, which is crucial for specific risk mitigation and prevention solutions. Forth, the effects of new, disruptive technologies on the situation of risk could be investigated from technical and managerial viewpoints, rendering the upcoming risk scenarios for anticipative actions.

ACKNOWLEDGEMENTS

This study is funded by the Tasmania Graduate Research Scholarship, iMOVE CRC and supported by the Cooperative Research Centres program, an Australian Government initiative.

REFERENCES

Alyami, H., Lee, P. T. W., Yang, Z., Riahi, R., Bonsall, S., & Wang, J. (2014). An advanced risk analysis approach for container port safety evaluation. *Maritime Policy & Management, 41*(7), 634-650. https://doi.org/10.1080/03088839.2014.960498

Årstad, I., & Aven, T. (2017). Managing major accident risk: Concerns about complacency and complexity in practice. *Safety Science, 91*, 114-121. https://doi.org/10.1016/j.ssci.2016.08.004

Aven, T. (2012). The risk concept-historical and recent development trends. *Reliability Engineering & System Safety, 99*, 33-44. https://doi.org/10.1016/j.ress.2011.11.006

Aven, T., & Heide, B. (2009). Reliability and validity of risk analysis. *Reliability Engineering & System Safety, 94*(11), 1862-1868. https://doi.org/10.1016/j.ress.2009.06.003

BIMCO. (2021, July 30). *The Guidelines on Cyber Security Onboard Ships*. BIMCO. https://www.bimco.org/-/media/bimco/about-us-and-our-members/publications/ebooks/guidelines-on-cyber-security-onboard-ships-v4.ashx

Bissell, K., Lasalle, R. M., & Cin, P. D. (2020). *Innovate for cyber resilience: Lessons from leaders to master cybersecurity execution.* Accenture.

Bjerga, T., Aven, T., & Zio, E. (2016). Uncertainty treatment in risk analysis of complex systems: The cases of STAMP and FRAM. *Reliability Engineering & System Safety, 156*, 203-209. https://doi.org/10.1016/j.ress.2016.08.004

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Cao, X., & Lam, J. S. L. (2019). A fast reaction-based port vulnerability assessment: Case of Tianjin Port explosion. *Transportation Research Part A: Policy and Practice, 128*, 11-33. https://doi.org/10.1016/j.tra.2019.05.019

Carlan, V., Coppens, F., Sys, C., Vanelslander, T., & Gastel, G. V. (2020). "Blockchain technology as key contributor to the integration of maritime supply chain?" In Vanelslander, T., and Sys, C. (Eds.), *Maritime Supply Chains* (pp. 229-259). Elsevier.

Chang, C. H., Xu, J. J., & Song, D.-P. (2015). Risk analysis for container shipping: from a logistics perspective. *The International Journal of Logistics Management, 26*(1), 147-171. https://doi.org/10.1108/Ijlm-07-2012-0068

Ellis, J. (2010). Undeclared dangerous goods - Risk implications for maritime transport. *WMU Journal of Maritime Affairs, 9* (1), 5-27. https://doi.org/10.1007/bf03195163

ENISA. (2019). *Port Cybersecurity: Good practices for cybersecurity in the maritime sector.* EU: European Union Agency for Cybersecurity (ENISA).

Fang, C., Marle, F., Zio, E., & Bocquet, J.-C. (2012). Network theory-based analysis of risk interactions in large engineering projects. *Reliability Engineering & System Safety, 106*, 1-10. https://doi.org/10.1016/j.ress.2012.04.005

Fruth, M., & Teuteberg, F. (2017). Digitization in maritime logistics—What is there and what is missing? *Cogent Business & Management, 4*(1), 1411066. https://doi.org/10.1080/23311975.2017.1411066

Garvey, M. D., Carnovale, S., & Yeniyurt, S. (2015). An analytical framework for supply network risk propagation: A Bayesian network approach. *European Journal of Operational Research, 243*(2), 618-627. https://doi.org/10.1016/j.ejor.2014.10.034

Global Maritime Issues Monitor. (2018, October 4). *Global Maritime Issues Monitor 2018.* Global Maritime Forum, Marsh, International Union of Marine Insurance. https://iumi.com/news/news/global-maritime-issues-monitor-2018-senior-maritime-stakeholders-deem-industry-not-prepared-to-deal-with-global-issues

Goerlandt, F., Khakzad, N., & Reniers, G. (2017). Validity and validation of safety-related quantitative risk analysis: A review. *Safety Science, 99*, 127-139. https://doi.org/10.1016/j.ssci.2016.08.023

Goerlandt, F., & Montewka, J. (2015a). A framework for risk analysis of maritime transportation systems: A case study for oil spill from tankers in a ship-ship collision. *Safety Science, 76*, 42-66. https://doi.org/10.1016/j.ssci.2015.02.009

Goerlandt, F., & Montewka, J. (2015b). Maritime transportation risk analysis: Review and analysis in light of some foundational issues. *Reliability Engineering & System Safety, 138*, 115-134. https://doi.org/10.1016/j.ress.2015.01.025

Goerlandt, F., & Reniers, G. (2018). Prediction in a risk analysis context: Implications for selecting a risk perspective in practical applications. *Safety Science, 101*, 344-351. https://doi.org/10.1016/j.ssci.2017.09.007

Greenberg, A. (2018, August 22). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History.* WIRED. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Gurning, S., & Cahoon, S. (2011). Analysis of multi-mitigation scenarios on maritime disruptions. *Maritime Policy & Management, 38*(3), 251-268. https://doi.org/10.1080/03088839.2011.572701

Heilig, L., & Voss, S. (2018). Port-centric information management in smart ports: A framework and categorisation. In Geerlings, H., Kuipers, B., and Zuidwijk, R. (Eds.), *Ports and Networks: Strategies, Operations and Perspectives* (pp. 236-250). USA: Routledge.

Ho, W., Zheng, T., Yildiz, H., & Talluri, S. (2015). Supply chain risk management: a literature review. *International Journal of Production Research, 53*(16), 5031-5069. https://doi.org/10.1080/00207543.2015.1030467

Ivanov, D., Dolgui, A., & Sokolov, B. (2018). The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. *International Journal of Production Research, 57*(3), 829-846. https://doi.org/10.1080/00207543.2018.1488086

Johnson, E. (2018, November 13). *Cyber-attack veterans, larger maritime companies best prepared.* The Journal of Commerce. https://www.joc.com/technology/veterans-cyber-attack-larger-maritime-companies-best-prepared_20181113.html?mgs1=a60aqyIopZ

Lam, J. S. L., &Bai, X. (2016). A quality function deployment approach to improve maritime supply chain resilience. *Transportation Research Part E: Logistics and Transportation Review, 92*, 16-27. https://doi.org/10.1016/j.tre.2016.01.012

Lee, C.-Y., & Song, D.-P. (2017). Ocean container transport in global supply chains: Overview and research opportunities. *Transportation Research Part B: Methodological, 95*, 442-474. https://doi.org/10.1016/j.trb.2016.05.001

Loh, H. S., & Thai, V. V. (2015). Managing port-related supply chain disruptions (PSCDs): a management model and empirical evidence. *Maritime Policy & Management, 43*(4), 436-455. https://doi.org/10.1080/03088839.2015.1107921

Manuj, I., & Mentzer, J. T. (2008). Global supply chain risk management strategies. *International Journal of Physical Distribution & Logistics Management, 38*(3), 192-223. https://doi.org/10.1108/09600030810866986

Nguyen, S. (2020). A risk assessment model with systematical uncertainty treatment for container shipping operations. *Maritime Policy & Management, 47*(6), 778-796. https://doi.org/10.1080/03088839.2020.1729432

Nguyen, S., & Wang, H. (2018). Prioritizing operational risks in container shipping systems by using cognitive assessment technique. *Maritime Business Review, 3*(2), 185-206. https://doi.org/10.1108/mabr-11-2017-0029

Nguyen, S., Chen, P. S.-L., & Du, Y. (2021a). Risk identification and modeling for blockchain-enabled container shipping. *International Journal of Physical Distribution & Logistics Management, 51*(2), 126-148. https://doi.org/10.1108/ijpdlm-01-2020-0036

Nguyen, S, Chen, P. S.-L., & Du, Y. (2021b). Container shipping operational risks: an overview of assessment and analysis. *Maritime Policy & Management, ahead of print (ahead of print)*, 1-21. https://doi.org/10.1080/03088839.2021.1875142

Nguyen, S., Chen, P. S.-L., Du, Y., & Thai, V. V. (2021c). An Operational Risk Analysis Model for Container Shipping Systems considering Uncertainty Quantification. *Reliability Engineering & System Safety, 209*, 107362. https://doi.org/10.1016/j.ress.2020.107362

Nguyen, S., Chen, P. S.-L., Du, Y., & Shi, W. (2019). A quantitative risk analysis model with integrated deliberative Delphi platform for container shipping operational risks. *Transportation Research Part E: Logistics and Transportation Review 129*, 203-227. https://doi.org/10.1016/j.tre.2019.08.002

Papathanasiou, A., Cole, R., & Murray, P. (2020). The (non-)application of blockchain technology in the Greek shipping industry. *European Management Journal, 38*(6), 927-938. https://doi.org/10.1016/j.emj.2020.04.007

Rae, A., & Alexander, R. (2017). Forecasts or fortune-telling: When are expert judgements of safety risk valid? *Safety Science, 99*, 156-165. https://doi.org/10.1016/j.ssci.2017.02.018

Rae, A., Alexander, R., & McDermid, J. (2014). Fixing the cracks in the crystal ball: A maturity model for quantitative risk assessment. *Reliability Engineering & System Safety, 125*, 67-81. https://doi.org/10.1016/j.ress.2013.09.008

Renn, O. (2008). White Paper on Risk Governance: Toward an Integrative Framework. In Renn, O., Walker, K. D. (Eds.), *Global Risk Governance* (pp. 3-73). Springer.

Rialland, A., & Tjora, Å. (2014). Future Internet enabled ship-port coordination. In Ehlers, S., Asbjørnslett, B. E., Rødseth, Ø. J., and Berg, T. E. (Eds.), *Maritime-Port Technology and Development* (pp. 217-226). London, UK: Taylor & Francis Group.

Sen, R. (2016). Cyber and Information Threats to Seaports and Ships. *In Maritime Security* (pp. 281-302). Elsevier.

Shi, X., & Chan, S. (2010). Information systems and information technologies for supply chain management. In Waters, D. (Eds.), *Global Logistics: New Directions in Supply Chain Management* (pp. 177-196). USA: Kogan Page Limited.

Sørensen, M. P. (2018). Ulrich Beck: exploring and contesting risk. *Journal of Risk Research, 21*(1), 6-16. https://doi.org/10.1080/13669877.2017.1359204

Thomas, M., Pidgeon, N., Whitmarsh, L., & Ballinger, R. (2016). Expert judgements of sea-level rise at the local scale. *Journal of Risk Research, 19*(5), 664-685. https://doi.org/10.1080/13669877.2015.1043568

Tsai, M.-C. (2006). Constructing a logistics tracking system for preventing smuggling risk of transit containers. *Transportation Research Part A: Policy and Practice, 40*(6), 526-536. https://doi.org/10.1016/j.tra.2005.11.001

Tseng, W.-J., Ding, J.-F., & Li, M.-H. (2013). Risk management of cargo damage in export operations of ocean freight forwarders in Taiwan. *Proceedings of the Institution of Mechanical Engineers, Part M: Journal of Engineering for the Maritime Environment, 229*(3), 232-247. https://doi.org/10.1177/1475090213513755

Tummala, R., & Schoenherr, T. (2011). Assessing and managing risks using the Supply Chain Risk Management Process (SCRMP). *Supply Chain Management, 16*(6), 474-483. https://doi.org/10.1108/13598541111171165

Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & Health Sciences, 15*(3), 398-405. https://doi.org/10.1111/nhs.12048

Van Der Sluijs, J. P., Craye, M., Funtowicz, S., Kloprogge, P., Ravetz, J., & Risbey, J. (2005). Combining Quantitative and Qualitative Measures of Uncertainty in Model-Based Environmental Assessment: The NUSAP System. *Risk Analysis, 25*(2), 481-492. https://doi.org/10.1111/j.1539-6924.2005.00604.x

Vilko, J., Ritala, P., & Hallikas, J. (2019). Risk management abilities in multimodal maritime supply chains: Visibility and control perspectives. *Accident Analysis & Prevention, 123*, 469-481. https://doi.org/10.1016/j.aap.2016.11.010

Wang, H., Tan, J., Guo, S., & Wang, S. (2018). High-value transportation disruption risk management: Shipment insurance with declared value. *Transportation Research Part E: Logistics and Transportation Review, 109*, 293-310. https://doi.org/10.1016/j.tre.2017.11.013

WEF. (2020). *Redesigning Trust: Blockchain Deployment Toolkit.* Switzerland: World Economic Forum.

Yang, Y. C. (2010). Impact of the container security initiative on Taiwan's shipping industry. *Maritime Policy & Management, 37*(7), 699-722. https://doi.org/10.1080/03088839.2010.524737

Yang, Y. C. (2011). Risk management of Taiwan's maritime supply chain security. *Safety Science, 49*(3), 382-393. https://doi.org/10.1016/j.ssci.2010.09.019

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. https://doi.org/10.1109/tr.2008.928208

Zio, E. (2018). The future of risk assessment. *Reliability Engineering & System Safety, 177*, 176-190. https://doi.org/10.1016/j.ress.2018.04.020