KR Maritime Cyber Safety News & Report

Vol. 061
March. 2024

Korean Register
www.krs.co.kr

CONTENTS

USCG Guidance on cyber security: A glossary of terms

Source : Safety4sea The Editorial Team

USCG has recently issued a Navigation and Vessel Inspection Circular (NVIC) to provide guidance for complying with reporting requirements for Breaches of Security (BOS), Suspicious Activity (SA), Transportation Security Incidents (TSI), and Cyber Incidents. The cyber incident guidance supports the reporting requirements and explains all related cyber security terms.

USCG highlights that any evidence of sabotage, subversive activity, or an actual or threatened cyber incident involving or endangering any vessel, harbor, port, or waterfront facility, including any data, information, network, program, system, or other digital infrastructure thereon or therein, shall be reported immediately.

The maritime industry continues to expand its use of networked technology, which creates efficiencies but also increases threats and vulnerabilities to MTS stakeholders and MTSA-regulated entities through telecommunications equipment, computers, and networks.

“Due to the increasing reliance on telecommunications equipment, computers, and networked systems for controlling physical operations, a growing portion of all security risks has a network or computer nexus. Maintaining the security of these systems, including reporting cyber incidents, is vital to maintaining the security of the MTS”

However, the USCG notes that routine spam, phishing attempts, and other nuisance events that do not breach a system’s defenses may not need to be reported as cyber incidents. Similarly, accidental violations of acceptable use policies, such as plugging in an unauthorized USB drive, is not considered a reportable cyber incident. Such occurrences, however, should be monitored for unusual activity such as escalation of efforts, and may be considered suspicious activities.

Norway takes measures to strengthen maritime cyber security

Source : Safety4sea The Editorial Team

Norwegian authorities have selected the Norwegian Maritime Cyber Resilience Centre (NORMA Cyber) to collaborate on cybersecurity within the maritime industry.

NORMA Cyber will play a crucial role in producing and distributing warnings, sharing information and vulnerabilities, and analyzing cyber incidents within the maritime sector, which includes ports, vessels, and shipowners, holding significant national and international importance.

Svein Ringbakken, Chairman of the board at NORMA Cyber, expressed satisfaction with the decision, highlighting the increased efforts to secure the maritime sector against a growing cyber threat. He emphasized the benefits for both society and the industry.

NORMA Cyber will closely cooperate with the Norwegian Coastal Administration (NCA) and the Norwegian Maritime Authority, with the assignment given by the NCA. The NCA, along with the Maritime Authority, serves as the maritime industry authority on security and preparedness, with the Ministry of Trade, Industry, and Fisheries assigning the Norwegian sectorial response environment for cybersecurity (SRM) to the NCA.

Lars Benjamin Vold, Managing Director of NORMA Cyber, welcomed the establishment of an SRM for the maritime industry, anticipating a more holistic approach to cybersecurity response and strengthened coordination with other industries.

NORMA Cyber will share vulnerability warnings, contribute to transparency and information sharing from cybersecurity incidents, and act as an advisory body during crisis and incident management. As part of its responsibilities, NORMA Cyber will join the NCA in relevant forums at the National Cyber Security Center (NCSC), increasing information access and maintaining the responsibility for information sharing within the maritime industry.

The tasks undertaken by NORMA Cyber will contribute to the crucial mission of securing the maritime sector, vital for Norwegian infrastructure, trade, and preparedness with its ports, vessels, and onshore facilities.

DCSA: Digital identity risks in container shipping

Source : Safety4sea The Editorial Team

DCSA has issued guidance on how to safeguard against financial crime with digital identity authentication and authorisation.

According to DCSA, as container shipping undergoes its digital trade transition, digital identity is a pivotal element. A digital identity functions as an online representation for individuals, organisations or devices, uniquely identifying and authenticating them in the digital realm.

The verification of digital identity, as this crucial online representation, is a vital business process. Its significance extends beyond mitigating risks such as data breaches and identity fraud. As DCSA finds, it also contributes to operational streamlining because:

- Digital identity verification allows for faster and more accurate processes. Automated checks on the identity of shippers, consignees and other stakeholders can reduce manual efforts and expedite onboarding procedures
- Digital identities enable the transition to paperless documentation. Electronic identification and authentication streamline the creation, verification and processing of shipping documents, reducing paperwork, minimising errors and accelerating document workflows
- Digital identity integration with tracking systems enables real-time visibility into the movement of goods. This transparency helps optimise logistics, improve route planning and enhance overall supply chain management.

In the shipping industry, the verification of the counterpart's digital identity takes on additional importance, particularly concerning sanction checks. These checks aim to identify and prevent transactions involving entities or individuals under sanctions or restrictions imposed by governments or international organisations, DCSA explains.

In 2020, the US Office of Foreign Assets Control (OFAC) issued a global advisory, encouraging those involved in transportation or trade in the maritime sector to conduct due diligence on documents suggesting cargo to and from high-risk areas for sanctions evasion.

As DCSA informs, this advisory, along with several others from various governing bodies, has expanded the scope of due diligence beyond mere paperwork compliance. Compliance teams are now tasked with assessing the risk profiles of all parties on the electronic bill of lading (eBL) in line with evolving regulations. This includes continuous checks of digital identities that might have become sanctioned.

Assuming responsibility, the shipping industry can safeguard itself from the economic repercussions of sanction evasion, including fines and reputational harm.

What do carriers and shippers need to know about digital identity?

Container carriers and shippers that exchange digital information with stakeholders must identify their communicating counterparts, validate they are who they claim to be, and authenticate their digital identities. Authentication in this context requires processes to reconfirm the identity of someone or something using credentials. In security terms, this process is commonly referred to as KYC or Know Your Customer.

KYC is a process that businesses use to verify the identity of their partners or customers. However, in the container shipping industry specifically, KYC may involve the verification of many more entities, DCSA notes. Amongst others, these include shippers and consignees, freight forwarders, shipping lines and carriers and financial institutions.

Verifying all the identities of all these entities for cybersecurity reasons is an important and ongoing process. But, in the context of the container shipping industry, KYC is crucial for several more reasons:

1. **Efficient operations:** KYC processes can streamline operations by ensuring that all necessary information about customers and partners is collected and verified continuously. This helps in reducing delays, errors and uncertainties in the shipping process
2. **Regulatory compliance:** many countries have regulations in place to prevent illegal activities such as money laundering, terrorism financing and sanctions violations. The shipping industry is subject to these regulations, and KYC helps companies ensure compliance with relevant laws. Only continuous monitoring of KYC data can ensure there are no violations. For example, sanctions checks can result in the prohibition of dealings with counterparts previously granted clearance
3. **Preventing fraud:** by verifying the identity of customers and partners, companies can prevent fraud and unauthorised access to sensitive information. This is particularly important in the

digital era, where transactions and communications often occur online. Data breaches can occur at all the endpoints of digital communication. Only monitoring of KYC data on an ongoing basis can ensure that information on file remains accurate

4. **Risk management:** KYC processes are essential for assessing and managing risks associated with customers and partners. Understanding who is involved in a transaction or a shipment allows companies to evaluate potential risks and act appropriately to mitigate them. For customers identified as high-risk, there may be a need to conduct enhanced due diligence (EDD) procedures. These may involve more in-depth verification of customer identity, source of funds and business activities.

KYC not only creates efficiency and ensures compliance with international regulations, it also fosters a transparent and trustworthy global trade environment, ultimately safeguarding the integrity of the container shipping industry, DCSA concludes.

IACS UR E26 and E27 applied to new ships contracted for construction on and after 1 July 2024.

Source : IACS

In an increasingly digitalised and interconnected world, where the maritime industry continues to adopt, at pace, new digital technologies, it remains imperative to focus on cyber threats and attacks that could compromise operations, safety and data integrity.

To address the need to enhance the cyber resilience of ships, last year IACS published UR E26 “Cyber Resilience of Ships”, and UR E27, “Cyber Resilience of On-Board Systems and Equipment”, which applied to new ships from 1 January 2024.

Since the publication of these requirements, and as experience of cyber security oversight in the maritime sector grows, the need for a standardized approach to survey requirements has been identified along with further enhancements resulting from industry feedback.

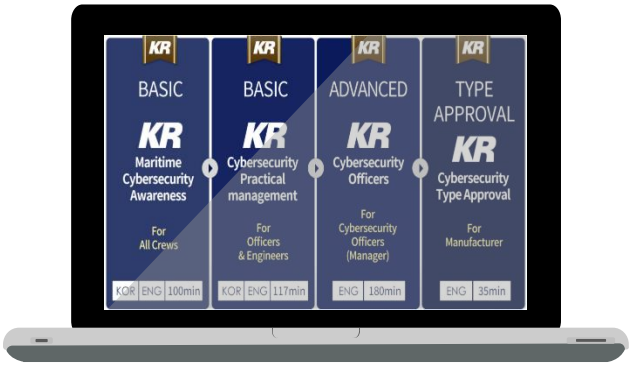
Additionally, and to address the challenges regarding the implementation of new cyber requirements in smaller and non-conventional vessels, the scope of applicability of these URs have been categorised as mandatory and non-mandatory compliance depending on vessel types and sizes.

These improvements have resulted in extensive changes to the two URs and so they will now supersede the originals and will be applied to **new ships contracted for construction on and after 1 July 2024.** To avoid confusion, the original versions, along with their previous application date of 1 Jan 2024, have been withdrawn. The revised version of UR E26 and E27 is available on the IACS website (https://iacs.org.uk/resolutions/unified-requirements/ur-e).

IACS Secretary General, Robert Ashdown, said ‘Incorporating industry feedback to ensure IACS requirements are clear in their applicability and are capable of being consistently applied in ship surveys, is important in ensuring that measures to enhance cyber resilience have the desired impact. As a result, and given that the original requirements had not yet entered into force, IACS has decided to apply only the revised requirements from 1 July 2024. It is believed that industry will welcome the clarity that this decision brings.’

Online Training

KR Maritime Cybersecurity e-Learning Center training course



Q&A : https://edu.orangecq.com/

KR reorganized the cyber security e-learning training in cooperation with Orange Security, who is a maritime cyber security specialist. Through this reorganization of e-learning training, KR becomes to provide customized training for each customer.

New curriculum consists of Maritime cyber security Awareness, cyber security Practical Management, cyber security Officers and cyber security Type Approval. Maritime cyber security Awareness is a course to raise awareness of maritime cyber security for employees including crews, which includes two modules - Understanding of Maritime Cyber Security and Practice of Maritime Cyber Security. cyber security Practical Management is a course for ship officers and engineers, which includes KR Remote Cyber Survey as well as Maritime cyber security Awareness course. cyber security Officers is for the person in charge of managing cyber security system and responding classification cyber security survey. This course consists of Administrative Security, Cyber Asset, Threat and Technical Security, Understanding of Maritime Cyber Security Risk Assessment with all modules in cyber security Practical Management. Finally, KR Cyber Security Type Approval is a course for equipment company and provides introduction of international standard related to requirements of cyber security for equipment and materials required for obtaining KR cyber security type approval.

KR CS++
KR Cybersecurity training tool

No.	Titles
1	Understanding of Maritime Cyber Security
2	Practice of Maritime Cyber Security
3	Administrative Security
4	Cyber Asset, Threat and Technical Security
5	KR Cyber Security Type Approval
6	Understanding of Maritime Cyber Security Risk Assessment
7	KR Remote Cyber Survey

KR has provided KR CS++, maritime cybersecurity training tool to the customers.

KR CS++ was produced in tablet type for effective cybersecurity training of seafarers in an environment where cybersecurity training is difficult due to the unstable Internet environment on ships. In addition, KR is striving for customer satisfaction by providing various types of services.

Currently, the same service is provided through cybersecurity e-learning education.

Providing the best services, Creating a better world

Cyber Certification Team, Korean Register
(46762) 36, Myeongji ocean city 9-ro, Gangseo-gu, Busan Republic ok Korea
Tel +82 70 8799 8595
Fax +82 70 8799 8594
www.krs.co.kr