KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 025

May 2020

KR Cyber security Activities #1

Maritime Cyber security training for Sun ace shipping

The Korean Register (KR) has delivered customized cyber security awareness training for Sun Ace Shipping. The maritime cyber security course sought to raise awareness amongst the company's employees. It included a general introduction to maritime cyber security, current status of maritime cyber threats and countermeasures, methods and actual cases of maritime cyber risk reduction, cyber asset list preparation and cyber risk evaluation practice. Information and appropriate methods to comply with IMO's resolution MSC.428(98) 'Cyber Risk Management in Safety Management System' were also covered. Customer feedback from the course praised the content as being valuable preparation for OCIMF inspections and the ISM Code cyber risk management. In particular, through the practice of evaluating cyber risk, feedback was received that it helped to strengthen cyber security capabilities. KR has conducted customized cyber security training so that domestic and overseas shipping companies such as Songa in UK, Sansho Korea, VL Enterprise PLC in Thailand can respond to OCIMF cyber security inspection and cyber risk management in the ISM code. The 'Understanding of Marine Cyber Security' course is included in the Education Support Project (MCF) which was organized by the Singapore Maritime Authority (MPA) in 2020 to provide training for Singapore shipping companies. In 2018, KR was designated as a "National Human Resources Development Consortium Education" operating agency, providing free training service on maritime cyber security awareness for domestic maritime workers. In the future, tailored cyber security education services will be offered to shipyards, equipment companies and shipping companies.

KR launches Cyber Security Service KR-CS++

Korean Register(KR, Chairman Lee Hyung-chul) announced that it has launched KR-CS++, a cyber security service brand. KR-CS++ is the meaning of ‘Beyond KR Cyber Security Service’. This service is intended to provide practical assistance for customers to implement the International Maritime Organization’s (IMO) resolution on cyber risk management (Resolution MSC428 (98)), which will take effect on January 1, 2021.

KR-CS ++ 2020, launched this time, includes training videos on cybersecurity awareness training and a commentary on cybersecurity practices. Cyber security awareness training video has been produced as a video for cyber security training service that KR has provided to domestic and foreign customers since 2017.

It consists of 'understanding maritime cyber security(https://youtu.be/fSIDLMj4gho)' and ‘practice of maritime cyber security management(https://youtu.be/67t0ckrNtiA)'.

'understanding maritime cyber security' is the contents for the cyber security awareness training of all employees, and it consists of the outline of maritime cyber security and cases of cyber accident. 'Practice of maritime cyber security management' is composed of the contents for practitioners and the method of cyber risk management. In addition, the Cyber Security Practice Commentary includes commentary for cyber security practitioners in companies and ships, and sample document forms that can be applied immediately to practice.

KR will include more cyber security education contents in KR-CS + + 2021 version in the future. It will develop services to help establish a maritime cyber security system more easily and provide it in the form of a smart pad.

MSC suffers website cyber attack

MSC suffers website cyber attack

Mediterranean Shipping Company (MSC), the world's second largest container shipping company, had to shut its website down from April 9th to 13th, for five days as a result of a malware cyber security attack. Fortunately, MSC was a holiday from the April 10th to the 13th because of Easter and COVID-19. it was reported that most of the employees were remote or telecommuting. The company's homepage is believed to have been targeted by malware, a software that infiltrated or damaged the system on 9 April. The cyber attack target was the company's Geneva headquarters, the IT system is separated between the head office and the agency, and the damage occurred only at the head office's data center. The IT systems of terminals, other departments and bases (depot) were unaffected and remained able to operate as normal.

The cyber attack was minimized by moving traffic to other online platforms intra, GT Nexus, cargo smart, or dialing. "Even with the suspension of some digital tools, all departments and terminals were able to respond to customers as usual, and the movement of cargo was no different than usual," the company said. Even so, it is widely believed that the cyber attack would still have caused a lot of damage to the company.

The cyber attack is the third on a global container shipping company: Maersk's trade volume, which was partially shut down by ransomware Notpetya in June 2017, fell by 20 percent. The estimated damage was between $250 million and $300 million. In July 2018, COSCO's American website and e-mail system were cyberattacked. The American network developed abnormalities, causing emails and telephone calls in the Americas to become paralyzed.

Source : http://www.cargonews.co.kr/news/articleView.html?idxno=43941

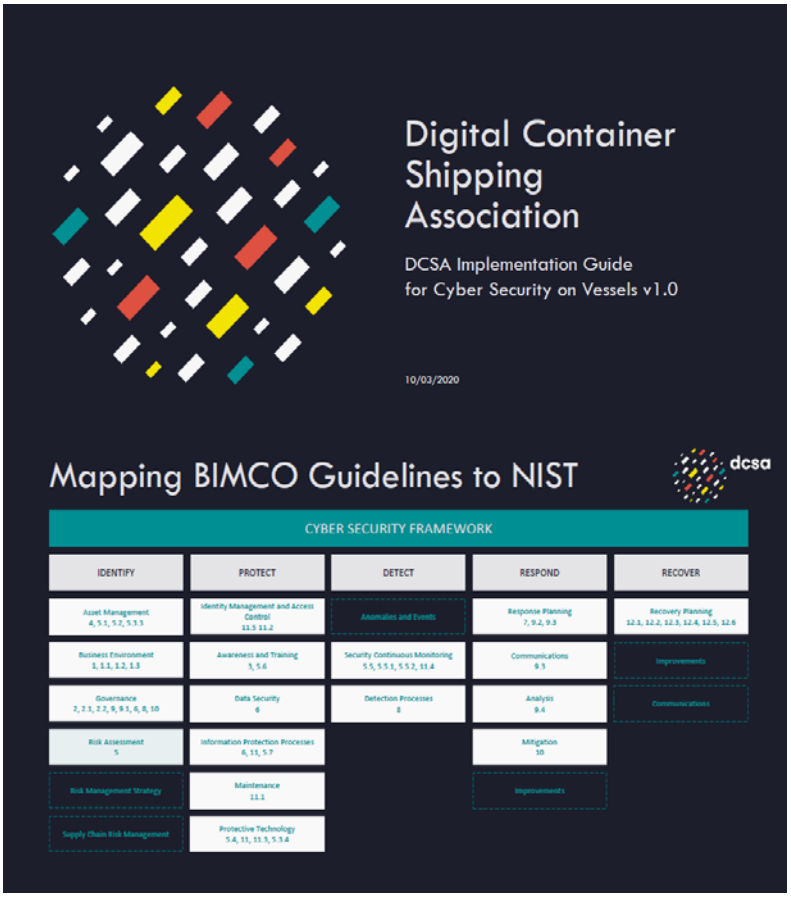
<Main screen situation exposed when accessing MSC homepage at 22:00 on April 11>

Source : http://www.dailylog.co.kr/news/articleView.html?idxno=20057#09sf

DCSA releases cyber security guidelines

DCSA releases cyber security guidelines

Nine major shipping companies, including Maersk line (Danish), MSC (Swiss), Hapag Lloyd (Germany), ONE (Japan), and Hyundai Merchant Marine (Korea), have established the Digital Container Shipping Association (DCSA) to digitize container transportation through technical standardization, and have announced the implementation of cyber security guidelines. The guidelines are said to be in advance of, and to prepare for the IMO Resolution MSC.428 (98) on maritime cyber risk management of the Safety Management System.



The guide is consistent with the existing BIMCO and NIST cyber risk management framework. It effectively integrates with the existing safety management system (SMS). It also provides templates to mitigate cyber threats on ships, prevent damage from cyber attacks, and to restore systems. To summarize the contents of the DCSA Cyber Security Implementation Guide, KR mapped the NIST functional elements to BIMCO's guidelines and the framework (identification, protection, detection, response, and recovery) defined in IMO MSC428(98). The DCSA provides non-technical explanations and specific measures to be taken to deal with each NIST element according to the level of cyber maturity of the company within each BIMCO framework. Under DCSA guidelines, the shipowner provides a template describing each vulnerability identified during cyber risk assessments, as well aligning a cybersecurity safety device catalog and remaining risks. The guidelines can be found free of charge on the DCSA website.

Source : DCSA Implementation Guide for Cyber Security on Vessels v1.0, 10/03/2020

Understanding Cyber Threats(OWASP Top 10 IoT)

Understanding cyber threats

A cyber threat is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, or the nation state through unauthorized access to an information system, causing destruction, disclosure, modification of information, and/or denial of service (source: NIST SP: 800-128). Cyber threats need to be categorized periodically to identify the vulnerabilities of assets, and the potential impact on that asset.

KR Guidance for Maritime Cyber Security System requirement(CS1)

204.1 Risk Management : External environmental factors affecting the environments of internal information technology and operational technology should be identified and cataloged as threats.

OWASP Top 10-Internet of Things(IoT)

The goal of the OWASP Things Internet Project is to help manufacturers, developers, and consumers understand more accurately the security issues associated with the Internet of Things and help users make wiser decisions in terms of security when building, distributing or evaluating IoT technology, according to the OpenWeb Application Security Project (OWASP). IoT)'s cyber threat Top10 and countermeasures are examined.

Top Ten	2014 IoT Top Ten	2018 IoT Top Ten
I1	Insecure Web Interface	Weak Guessable, or Hardcoded Passwords
I2	Insufficient Authentication/Authorization	Insecure Network Services
I3	Insecure Network Services	Insecure Ecosystem Interfaces
I4	Lack of Transport Encryption	Lack of Secure Update Mechanism
I5	Privacy Concerns	Use of Insecure or Outdated Components (NEW)
I6	Insecure Cloud Interface	Insufficient Privacy Protection
I7	Insecure Mobile Interface	Insecure Data Transfer and Storage
I8	Insufficient Security Configurability	Lack of Device Management
I9	Insecure Software/Firmware	Insecure Default Settings (NEW)
I10	Lack of Physical Hardening	Poor Physical Security

Source : OWASP Top 10 Project

Insecure ecosystem Interfaces

An unsafe web, backend API, cloud or mobile interface in an ecosystem outside the device can damage the device or associated components. Common problems include a lack of authentication/authority, lack of encryption or vulnerability, lack of input and output filtering. The following table gives examples of security measures for the "unsafe ecosystem interface" as recommended by ENISA (European Network and Information Security Agency).

DOMAIN	SECURITY MEASURE	THREAT GROUP	REFERENCE
Security by design	interfaces and communication security	· Outages · Legal · Disaster	· ISO - ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls · NIST - NIST SP 800 53r4: Security and Privacy Controls for Federal Information Systems and Organizations
Cloud Security	Protect all the data within the cloud and data in transfer. Ideally, all data should be encrypted. Application and interfaces should be secured as well.	· Nefarious activity / Abuse · Eavesdropping / Interception / Hijacking	· IEC - IEC 62443-2-1:2010 Establishing an industrial automation and control system security program · ISO - ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements · NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security
Access Control	Implement in the device and/or use an account lockout functionality that activates after the number of failed login attempts exceeds the value of a set parameter. This also applies to cloud and mobile interfaces. Develop a policy to specify details such as the number of allowed attempts and time of the lockout.	· Nefarious activity/Abuse	· IEC - IEC 62443-3-3:2013 System security requirements and security levels
Networks, protocols and encryption	Ensure security of communications channels related to IIoT solutions. Encrypt communications in case of important data (e.g. configuration, personal data, data for control purposes), where it is possible to do so without affecting safety, availability and performance.	· Eavesdropping / Interception / Hijacking	· NIST - NIST SP 800 82r2: Guide to Industrial Control Systems (ICS) Security

Source : ENISA, Good Practices for Security of Internet of Things, NOVEMBER 2018

Understanding Guideline for Type Approval of Maritime Cyber Security

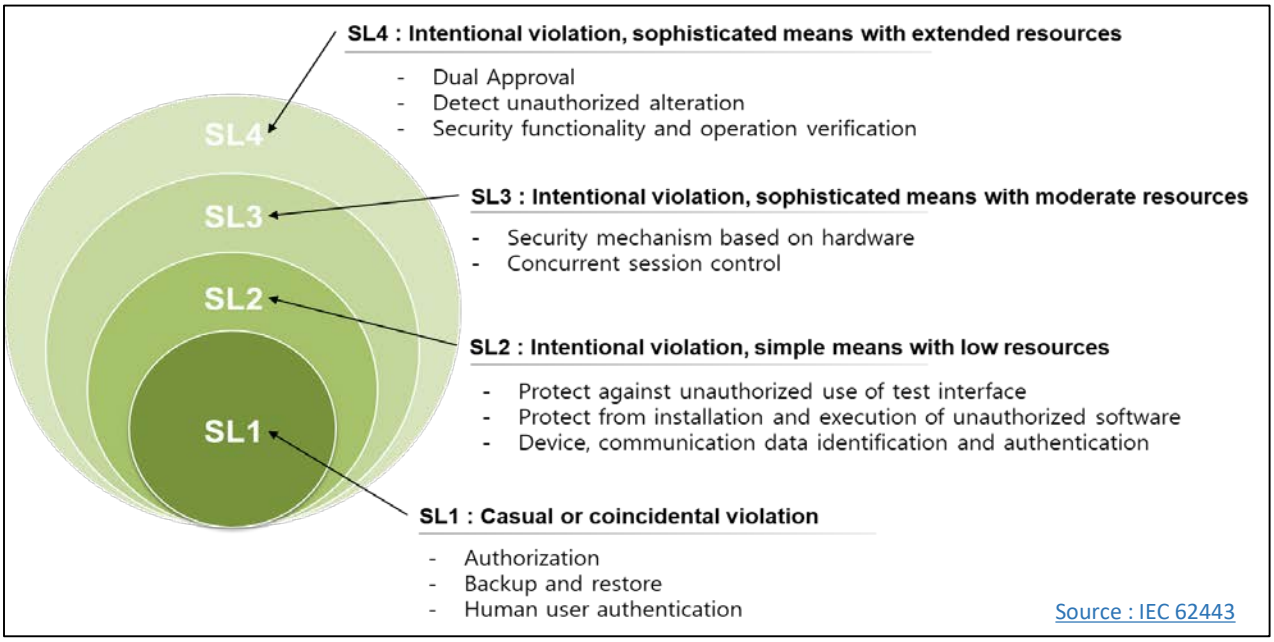
Type approval is to certify for the manufacturers of equipment for marine use that equipment comply with the provisions for the type approved products in the Guidance, where deemed satisfactory by the Society as the results of carrying out the examination, tests and inspection specified in the Guidance before installation on board. The cyber security type approval has been developed based on international standards such as ISA 62443 4-2, IEC 61162-460, and inspect cyber security level and function of cyber systems including remote access equipment, integrated control and monitoring systems on board the ship. The security requirements and their levels are verified on 12 categories and 124 requirements.

< Composition of KR Cyber Security Type Approval Guidelines >

Section 1 General	Section 5 Data Confidentiality	Section 9 Software Application Requirements
Sections 2 Identification and Authentication	Section 6 Restricted Data Flow	Section 10 Embedded Device Requirements
Section 3 Use Control	Section 7 Timely Response to Events	Section 11 Host Device Requirements
Section 4 System Integrity	Section 8 Resource Availability	Section 12 Network Device Requirements

Source : http://www.krs.co.kr/KRRules/KRRules2019/data/data_other/ENGLISH/gc31e000.pdf

Understanding Security Level (SL)



Source : IEC 62443

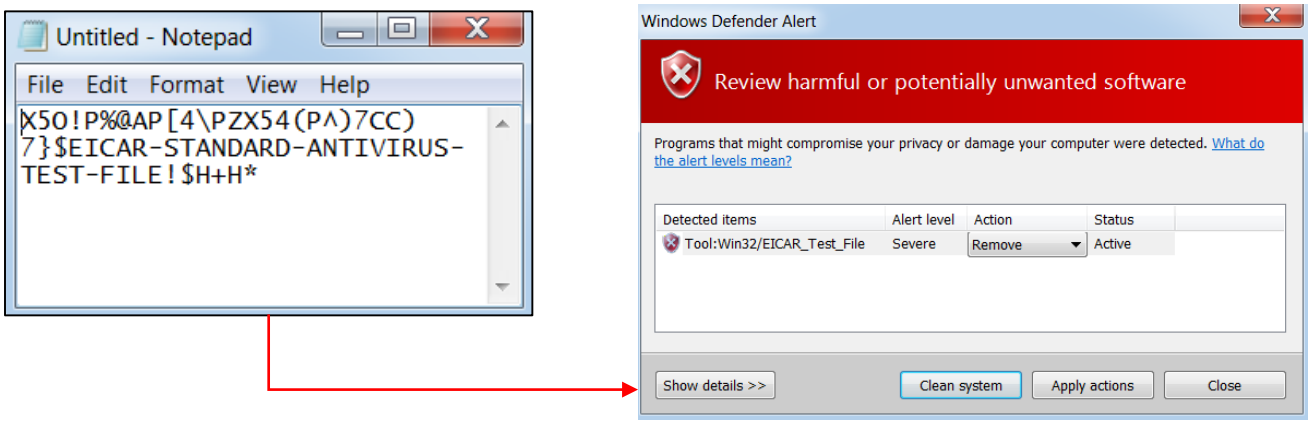
KR Type Approval of Maritime Cyber Security Inspection Items

Security functionality verification (402)

1. Components should provide the capability to support verification of the intended operation of security functions according to ISA 62443-3-3 SR 3.3.(SL 1,2,3)
2. Components should provide the capability to support verification of the intended operation of security functions during normal operations.(SL 4)

Security function verification based on EICAR test file

The product supplier and/or system integrator should provide guidance on how to test the designed security controls. Asset owners need to be aware of the possible ramifications of running these verification tests during normal operations (Source: IEC 62443 4-2). One of the way verifying the security function is using an EICAR (European Institute for Computer Antivirus Research) test file for anti-virus vaccine.



< Example of security function verification with EICAR test file>

When writing the following sentence on a notepad and saving it, if an anti-virus vaccine is installed and working properly, the text file is detected as a virus and anti-virus vaccine will perform a predefined action (eg, generating a warning or alarm, deleting text file, etc.).

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

(Source: www.eicar.org)

Cyber security type approval verifies the security functions predefined by the product supplier and verifies that they are provided. In order to meet SL4 requirement, verification of security function should be done without interruption of system normal operation.

Explanation of Term

DCSA

- Digital Container Shipping Association (DCSA) was founded in four major shipping companies in the world, including Maersk Line, MSC, Hapag-Lloyd, and ONE. It was created for data standardization work to overcome inefficiency caused by data formats, and recently distributed cyber security guidelines.

Malware

- Malware is software designed to invade or damage computer systems without the owner's consent. Once installed, it is very difficult to remove and it is designed to simplify the installation of the program. The results of this work may be classified as a little annoying, and in some cases, irrecoverable damage may cause the owner's hard drive installation to be inconvenient. Examples of malware are viruses or Trojan horses [WIKI]

Ransoware

- Ransomware is a type of malicious software that infects a computer system, restricts access, and demands some kind of ransom. Because access to the computer is restricted, to remove the restriction, the person who developed the malicious program is forced to pay. At this time, there is a ransomware that is encrypted, while some simply lock the system and prompt the computer user to pay [WIKI]