KR Maritime Cyber Security

News from KOREAN REGISTER

Aug 2018

Vol. 004

KR Maritime Cyber Security Activity

● Ship Cyber Security Survey

On July 29, as a part of the technical consulting service for Songa Shipmanagement, SONGA HAWK on-board cyber security survey was performed. Major check points are as follows,

- OCIMF SIRE VIQ cyber security pre-audit and providing guideline
- Identify the improvement measures of ship risk assessment
- KR cyber security checklist based survey : PC security vulnerability diagnosis

In this survey, cyber security surveyor checked physical security (KR Maritime cyber security management system guidance : CSMS 1 207) based on classification checklist and executed application program for PC security vulnerability diagnosis including periodic change of password and screen saver setting time.

Korean Register is expected to improve reliability of classification cyber security by providing guideline for enhancing ship cyber security to ship owners based on their proficient knowledge and experience. Also, it is expected to improve technical survey skills through the practical application program such as PC security vulnerability diagnosis.

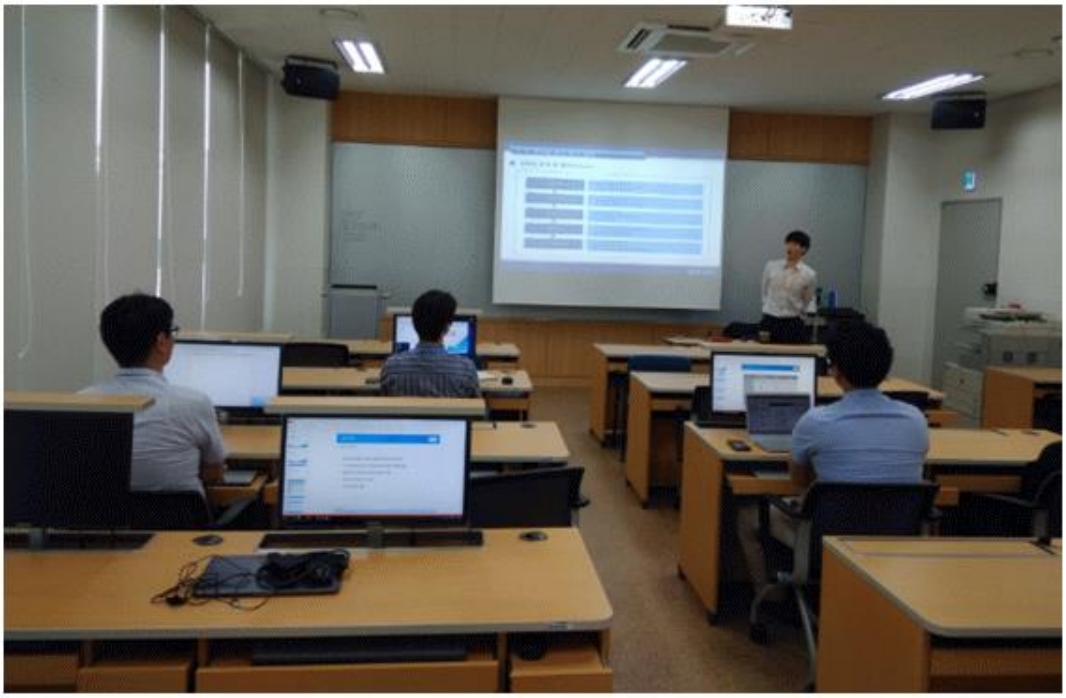
● Cyber Security Surveyor Training

On July, Korean Register conducted training for cyber security surveyor to enhance technical understanding of cyber security inspection and to perform actual ship and company inspection. The training was five days and the curriculum is as follows.

Date	Contents	Details
7.19 – 7.20	Technical security	- PC vulnerability diagnosis - Penetration test overview
7.23	Administrative security	- Cyber security awareness - KR yber security notation
7.24 – 7.25	KR Cyber security survey	- Cyber asset identification - Cyber security risk assessment

In particular, it is expected that PC vulnerability diagnosis and penetration test training will be helpful to surveyor for ship and company cybersecurity inspection.

In addition, the "Maritime Cyber Security Overview" and "Maritime Cyber Security Management Practice" course will be offered for employees and staff members working in the maritime industry (shipping companies, shipyards, equipment manufacturers) on September and October.



● 2018 KR Southeast Asian Technical Seminar

Korean Register held 'KR Singapore Technology Seminar' and 'KR Bangkok Technology Seminar' in Southeast Asian maritime industry in Singapore and Bangkok on July. More than 200 people attended the KR Singapore Technology Seminar held on the 26th, including Navig8, Bernhard Schulte and other shipping companies and officials from the Singapore Maritime Service. In addition, Lloyd's List and Fairplay, which are representative world shipping magazines, also showed interest. In addition, more than 70 participants from the maritime industry including shipping companies such as Thoresen & Co., Precious Shipping Public and Nathalin Management, shipyards and Thai shipowners' associations attended the seminar of KR Bangkok Technology held on 24th.

In this technical seminar for the Southeast Asian maritime industry, Korean Register presented IMO's Global Sulfur Cap trend and maritime cyber security, and also introduced KAMSARMAX bulk ship design.

Lee Jeong ki, the Chairman & CEO of KR, said, "Recently, the global maritime industry faces more challenges than ever before, including environmental regulations and cyber threats. In this context, we organized seminars to share the latest trends and responses of maritime industry. "

COSCO Network down by Cyber Attack

Following Maersk Line ransomware infection in June 2017, there was also an infection that was known as NotPetya at COSCO Shipping, which is the fourth largest in Chinese country.

● America Region Network Down

According to several media, COSCO only disclosed the fact that it was a network down in the America region without directly mentioning the ransomware infection. However inside the company, it is strengthening system and network that prevents spread of malware along with warning of harmful email. The company said, "E-mail and telephone services are not being restored in the America region, but the operation of COSCO ships worldwide is normal, and the core operating system of the business is also operating safely". In particular, after the accident, the company released a 6-page emergency response document due to a failure in the U.S. area network down and released temporary external e-mail addresses, such as Yahoo and Gmail, to communicate with cargo schedule and invoice processing.

(Frequently Asked Questions about Network Problem within America Area)

● NotPetya Ransomware Infection

NotPetya, which is known to have infected COSCO systems, not only COSCO, but also infected Mask Line's systems and Fedex, a logistics system, in 2017, which resulted in damage of about $ 300 million each. Furthermore, it was the main cause of widespread damage to many companies located in Ukraine. NotPetya is a variant of Petya that uses Windows SMB(server message block) vulnerability to encrypt full MBR(Master Boot Record) files, and requires bit coins at the cost of decryption. NotPetya, unlike Petya, may not be able to recover encrypted data at its source.

In particular, the crucial difference between the NotPetya and Petya is that it can propagate itself without user intervention, meaning it can cause even greater damage.

● A lot of time to pinpoint the damage

Although the damage of COSCO is expected to be smaller than that of Maersk Express or FedEx in 2017, it will take a considerable amount of time to figure out the exact extent of the damage. According to a media, it expects restoration to be 4,000 servers, 45,000 PCs, and 2,500 applications. Other media predicted that the specific extent of the damage would become clearer after the fiscal year.

Response and Suggestion

A Petya / NotPetya operating in a Windows system environment exploits Server Message Block (SMB) vulnerabilities, a form of messages used to share files, directories and peripherals. It was released security patch in May 2017. The subjects covered were Windows XP, Windows 7, Vista, 8, etc, and Windows 10 was not included in the damage. Companies using Windows Server or PC without security patches should apply the security patches quickly and, if necessary, update the operating system.

Ref. : **COSCO Ransomware Spreads, Hazardous Cargo Bookings Cancelled,** Computer Business Review, July, 2018

Cyber, Climate Risks and Human Error Threaten Shipping's Safety Progress

The shipping logistics loss has been steadily declining to 38% the past decade, but the risk of cyber security, climate risks and human error are expected to be a stumbling block to the trend.

● Leading to cyber security law enforcement

According to the report, Allianz Global Corporate & Specialty's, 'Safety & Shipping Review 2018', the positive trend of reducing losses in the maritime logistics sector is expected to continue. However with the increased use of new shipbuilding technology, the portion of the losses will also undergo changes. In particular, malicious code such as NotPeyta explains how important cyber security threats are in the logistics sector, and that guidelines such as NIS enforce compliance to shippers.

● Human Error: Still a big issue. Data can help

With cybersecurity, there was also a question of human error. According to the report, despite repeated improvements over the past several years, improvements in human error have not been satisfactory, and significant amounts of data have been compiled by shipping companies. In addition, losses due to climate change were cited as the main culprit of ocean accidents.

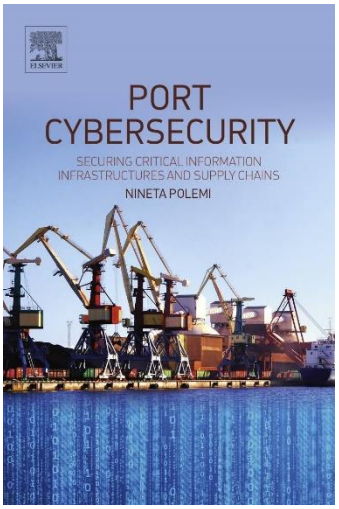
Response and Suggestion

Along with the maritime logistics sector, IT dependence on shipping will continue to rise, leading government agencies to expect cybersecurity requirements to be enhanced in both ships and logistics IT. The owners and the shipping company are required to prepare for the ongoing flow of cyber security requirements by continent and country.

Ref : Cyber, Climate Risks and Human Error Threaten Shipping's Safety Progress, Business Wire, July, 2018

Port Cyber Security

'Port Cybersecurity', published in October 2017, said port security focused on physical security should consider cybersecurity standardization and legal requirements along with ICT developments According to Nineta Polemi, the author of the book, ISPS should be considered as well as cybersecurity, which will follow suit to new legal frameworks.



● CIIP Directive eIDAS, NIS Directive

In SearchSecurity, Nineta Polemi mentioned various security regulations, including the following :

- **CIIP Directive (2012),** critical information infrastructure protection: toward global cybersecurity;
- **The Cybersecurity Strategy for the European Union (2013) and the European Agenda on Security (2015)** provide the overall strategic framework for the EU initiatives on cybersecurity and cybercrime;
- **eIDAS Regulation (2014)** on electronic identification and trust services for electronic transactions in the internal market;
- **NIS Directive (2016)** applies only to those public administrations that are identified as operators of essential services;
- **cPPP Initiative (2015)** ensures that Europe will have a dynamic, efficient, and effective market in cybersecurity products and services;
- **Enhanced Privacy Directive (2016),** mandatory reporting of security breaches;
- **USA H.R. 3878, House of Representatives**, "Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2015."

In addition, ISO/IEC 27001 and Risk Management related series (ISO/IEC 27005, ISO/IEC 27005), which are essential requirements for cybersecurity, are also to be considered as cybersecurity standards.

Response and Suggestion

Cyber security incidents that occurred in the maritime sector in 2017 are also an opportunity to strengthen cyber security requirements in port areas of each country. These legal requirements should be prepared for legal performance as they are likely to be applied to all vessels approaching the port.

Ref. Port Cybersecurity, TechTarget, July, 2018

Understanding Cyber Threat

● Understanding cyber threat

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

● KR Guidance for Maritime Cybersecurity Management System requirement (CSMS1)

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

● BSI top 10 cyber threat

Threats to ICS are due to attacks or events that could potentially damage ICS and its related businesses due to existing vulnerabilities. The following table lists the most serious threats to ICS published by the German Federal Information Security Agency. Following the newsletter in July, we will analyze the "Intrusion via remote access" of the BSI 10 cyber threats.

No. (old No.)	Top 10 2016	Top 10 2014
1 (3)	Social Engineering and Phishing†	Malware Infection via Internet and Intranet
2 (2)	Infiltration of Malware via Removable Media and External Hardware	Infiltration of Malware via Removable Media and External Hardware
3 (1)	Malware Infection via Internet and Intranet	Social Engineering
4 (5)	Intrusion via Remote Access	Human Error and Sabotage
5 (4)	Human Error and Sabotage	Intrusion via Remote Access
6 (6)	Control Components Connected to the Internet	Control Components Connected to the Internet
7 (7)	Technical Malfunctions and Force Majeure	Technical Malfunctions and Force Majeure
8 (9)	Compromising of Extranet and Cloud Components	Compromising of Smartphones in the Production Environment
9 (10)	(D)DoS Attacks	Compromising of Extranet and Cloud Components
10 (8)	Compromising of Smartphones in the Production Environment	(D)DoS Attacks

Ref. : Industrial Control System Security – Top 10 Threats and Countermeasures 2016

● BSI top 10 cyber threat : Intrusion via remote access

External access for maintenance purposes is very common in ICS installations. Poorly secured access e.g. via default passwords or even hardcoded passwords is a widespread issue. The respective product suppliers and external service providers are often contracted for maintenance and programming of components. This creates additional challenges for security management as it requires harmonization of the security concepts of several parties.

<Potential threat scenarios>

▣ Direct attack on an maintenance access point, e.g. by

- a brute-force attack on password-protected access points,
- web-specific attacks, e. g. injection or CSRF, on access points used for maintenance.

▣ Indirect attack via the IT systems of the service provider the external access was created for, e.g.

- trojans exploiting the access directly on the external maintenance computer,
- theft of passwords, certificates or other tokens or other ways of aquiring login details, e. g. by bribing / blackmailing staff possessing such privileges,
- use of stolen notebook computers with software configured for external access.

<Countermeasures>

- Default users / passwords of a product supplier (delivery condition) should be deactivated, blocked or deleted (acceptance protocol).
- Use of sufficiently secure authentication procedures, e. g. pre-shared keys, certificates, hardware tokens, one-time passwords and multi-factor authentication through possession and knowledge.
- Protection of the transmission route by encryption, e. g. SSL/TLS.
- Sufficiently granular segmentation of networks to minimize the “reach“ of remote access.
- Setup of access points for remote maintenance in a demilitarized zone (DMZ), so that service providers first connect to a DMZ instead to the ICS network and obtain the required access on the target system only from there.
- Enabling of remote access by internal personnel only for duration and the purpose of remote maintenance.

Ref. : Industrial Control System Security – Top 10 Threats and Countermeasures 2016

Guideline for Cyber Risk Assessment

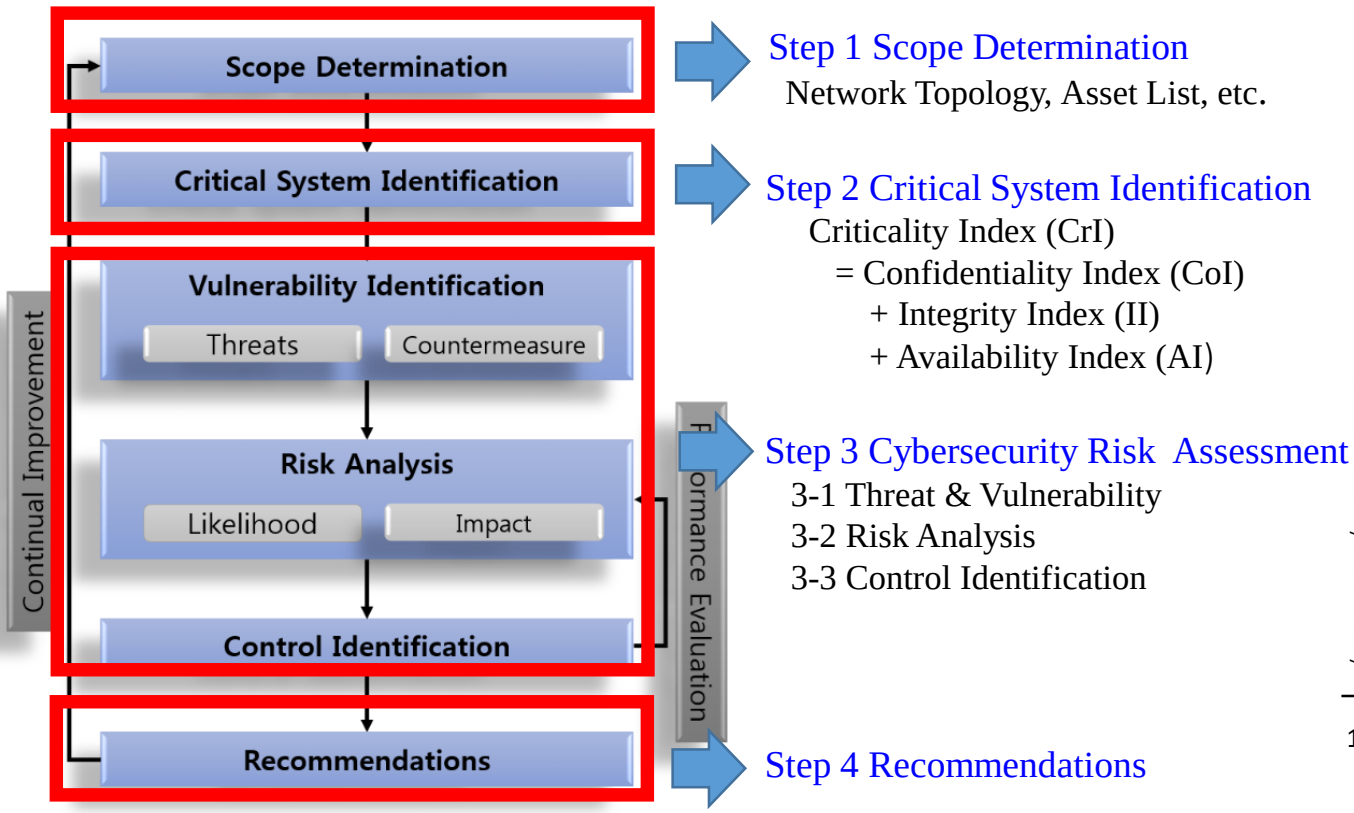
● The need for cyber risk assessment

Cyber risk assessment is needed to protect ship and company assets from cyber threats and to continuously improve and manage cyber security. Structured and systematic risk assessment methodologies should be used to identify vulnerable areas of the ship and companies key systems and to reduce cyber risks to enhance cyber security. Through systematic cyber security risk assessment, a strategic decision should be made to check the cyber security risk level for the main system of the ships and companies and to analyze the gap with the targeted risk level to improve the level of cybersecurity.

● **KR Guidance for Maritime Cybersecurity Management System requirement (CSMS1)**

> **204.4 Risk Management :** Risk assessment should be periodically carried out by linking the threat identification and vulnerability diagnosis results to all assets.

● KR Cyber Security Risk Assessment Process : 4 Step



● **STEP 1 : SCOPE DETERMINITATION**

Objective : To understand purpose & scope of risk assessment and risk criteria clearly by gathering the required information

Preliminaries : Network topology, Asset list, Risk acceptance criteria

● **STEP 2 : CRITICAL SYSTEM IDENTIFICATION**

Objective : Identify critical systems by analyzing the impact of assets (results) on business activities

Preliminaries : Asset assessment through CIA (refer to July newsletter guideline)

● **STEP 3 : CYBER SECURITY RISK ASSESSMENT**

Objective : Identify threats to critical systems, create cyber attack scenarios, identify risk levels, and make improvements to reduce risk through workshops

Preliminaries : Threat list, Workshop

● **STEP 4 : RECOMMENDATION**

Objective : Document the result of the cyber security risk assessment(level of cyber security risk, improvement actions to reduce risk, responsible person)

Impact	5	5 Significant	10 Significant	15 Major	20 Major	25 Major
	4	4 Low	8 Significant	12 Significant	16 Major	20 Major
	3	3 Low	6 Significant	9 Significant	12 Significant	15 Major
	2	2 Low	4 Low	6 Significant	8 Significant	10 Significant
	1	1 Low	2 Low	3 Low	4 Low	5 Significant
Index		1	2	3	4	5
		Probability				

Cybersecurity Risk = (Threat x Vulnerability) x Consequence

Ref. : IEC 62443, ISO 2705 : 2011, API STD 780

Explanation of term

- **SMB(Server Message Block) Vulnerability :** A message format (protocol) used to share files or directories and peripherals within the Windows operating system. Although the initial Microsoft standard, it is convenient to share files and peripherals, making it a protocol in the course of Windows compatibility for operating systems such as UNIX and Linux. However, there have been many security vulnerabilities in this protocol, as the server responds to certain requests. Petya, Warner Cry Ransomware and others were also abused through the vulnerabilities.
- **MBR(Mater Boot Record) :** It is a special type of boot sector at the very beginning of partitioned computer mass storage devices. Simply, if the area of the system where the hard disk was first written is destroyed or corrupted, the PC or System will not work and often will not boot.
- **Security Patch :** A patch is a set of changes to a computer program or its supporting data designed to update, fix, or improve it. This includes fixing security vulnerabilities and other bugs, with such patches usually being called bug fixes or bug fixes and improving the usability or performance.
- **ISO/IEC 27001 :** An international standard that specifies requirements for the Information Security Management System(ISMS) established by the ISO(International Standard Organization). Based on BS7799, a British standard in 2005, it contains standards for corporate risk management, security policy and asset management for information protection.
- **DMZ(Demilitarized zone) :** Refers to a neutral area in a network and a space separated from the internal network for protecting internal resources when providing services to the outside. In other words, the internal network can be protected from the intrusion of servers in the DMZ by placing a section called DMZ between the internal network and the external network.