KR Maritime Cyber Security

News from KOREAN REGISTER

Dec 2018

Vol. 008

KR Cyber Security Activities

- Kormarine Conference 2018

Global Maritime Issues Monitor 2018

ISF Forecasts 2019 Global Security Threat

Guidelines for Updating Anti-virus Program on OT System onboard of Ships

Cybersecurity Issues and Countermeasures for OT system onboard of Ships

Understanding of Cyber Threats

- Extranet and Cloud Component Damage

Guidelines of Establishing Access Control Policy

Explanation of Term

KR Cyber Security Activities

● Kormarine Conference 2018

Korean Register participated Kormarine Conference 2018 held at the Haeundae Grand Hotel in Busan from Nov. 20 to 21 and announced major concerns in maritime industry, including cyber security, sulfur oxides, etc.

Komarine Conference, organized by the Ministry of Trade, Industry and Energy and the Busan Metropolitan City and sponsored by Korea Marine Equipment Association, under the theme of “Ask the New Way to the Shipbuilding and Marine Industries” covered the trends of the shipbuilding and marine equipment industries following changes in environmental regulations with domestic and foreign 25 speakers.

Yeon-Tae Kim, Senior Vice President of Korea Register, headed the first session, and led the discussion on the latest technologies in the maritime industry, including autonomous ships, LNG fueled propulsion ships and cyber security. In this session, Kae-Myoung Park, General Manager of Cybersecurity TFT, shared best practices of cyber security and forecast based on his experience in establishing cybersecurity management systems for domestic and foreign companies. Hyun-Tae Kim, Senior Surveyor of Korean Register, discussed the environmental regulations of the International Maritime Organization (IMO), including SOx regulation and the meeting result of 73rd Marine Environmental Protection Committee (MEPC), in the second session. (www.kormarineconferences.org)

Global Maritime Issues Monitor 2018

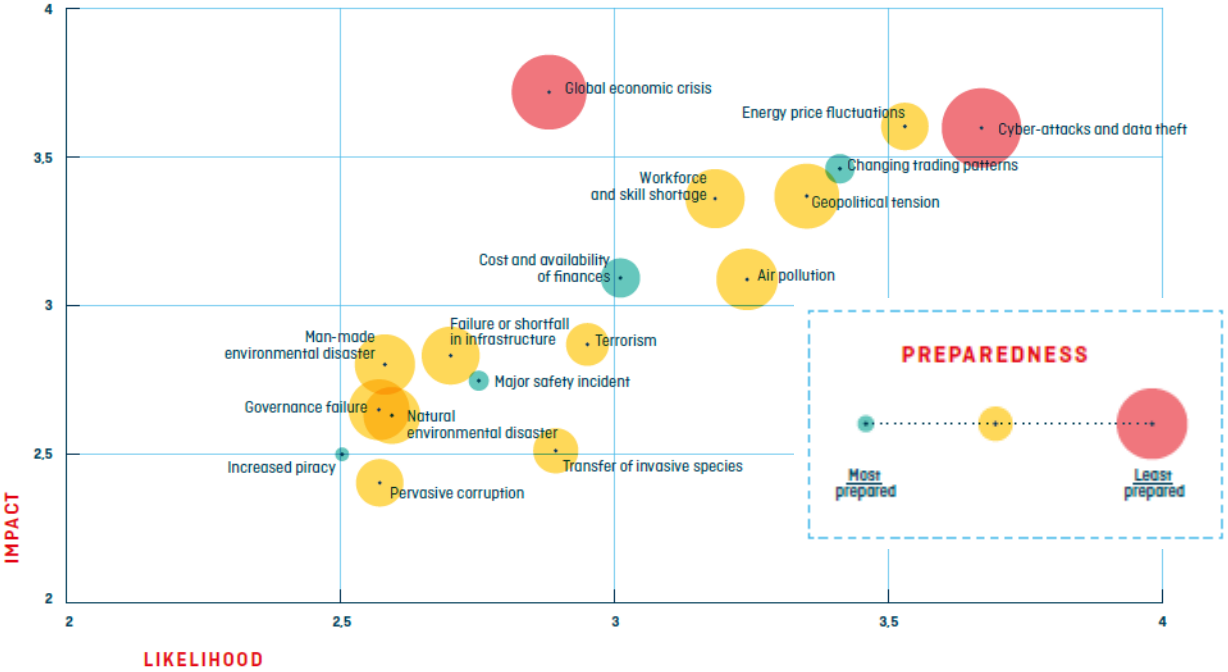
● ‘Cyber attacks and data theft’ have the most impact

According to the Global Maritime Issues Monitor 2018 report provided by the Global Maritime Forum in Hong Kong on October 3, a survey of major marine stakeholders in more than 50 countries found that ‘**Cyber attacks and data theft’** is likely to have the largest impact on the 17 major global issues over the next decade. The rankings were estimated in terms of impact, likelihood and preparedness for a number of issues potentially affecting the global marine industry.

1) Impact : The top three issues that are considered to have the greatest potential impact in the maritime sector are the global economic crisis (1), energy price fluctuations (2), cyber attacks and data theft (3).

2) Likelihood : The top three issues considered most likely to occur within 10 years were cyber attack and data theft (1), energy price fluctuations (2), and changing trading patterns (3).

3) Preparedness : The top three issues considered lacking in preparation were cyber attack and data theft (1), the global economic crisis (2), and geopolitical tension (3).



Ref. : Global Maritime Issues Monitor 2018

ISF Forecasts 2019 Global Security Threat

● Four security threats that business will face in 2019

The Information Security Forum (ISF) has announced the organization's outlook for the top global security threats that businesses will face in 2019. Key threats for the coming year include:

- **The Increased Sophistication of Cybercrime and Ransomware :** Criminal organizations will continue their ongoing development and become increasingly more sophisticated. In 2019, attacks on personal smart devices, such as mobile malware and mobile Ransomware, are expected to increase.
- **The Impact of Legislation :** Organizations have insufficient knowledge and resource to keep abreast of current and pending legislation. In addition, the law is dominated by governments and regulators in nature, and is shifting to national regulation when cross border collaboration is needed. Organizations will try to keep up with changes that can affect their business models.
- **Smart Devices Challenge Data Integrity :** Organizations will use smart devices without realizing they provide many opportunities for attackers due to design insecurity. Also, there will be an increase in the lack of transparency of the IoT where corporate data can be used in ways that customers do not intend. It is problematic for businesses to know what information will be leaked or secretly captured and transmitted by devices like smart phones, smart TVs. When transparency violations are revealed, organizations will held liable by regulators and customers for inadequate date protection.
- **The Myth of Supply Chain Assurance :** The supply chain is a vital component of global business operations for all organizations and today's global economy. However, a range of valuable and sensitive information is often shared with suppliers, and when that information is shared, direct control is lost. In 2019, organizations will discover that assuring the security of their supply chain is a lost cause and instead, it is time to refocus on managing their key data and understanding where and how it has been shared across multiple channels and boundaries, irrespective of supply chain provider.

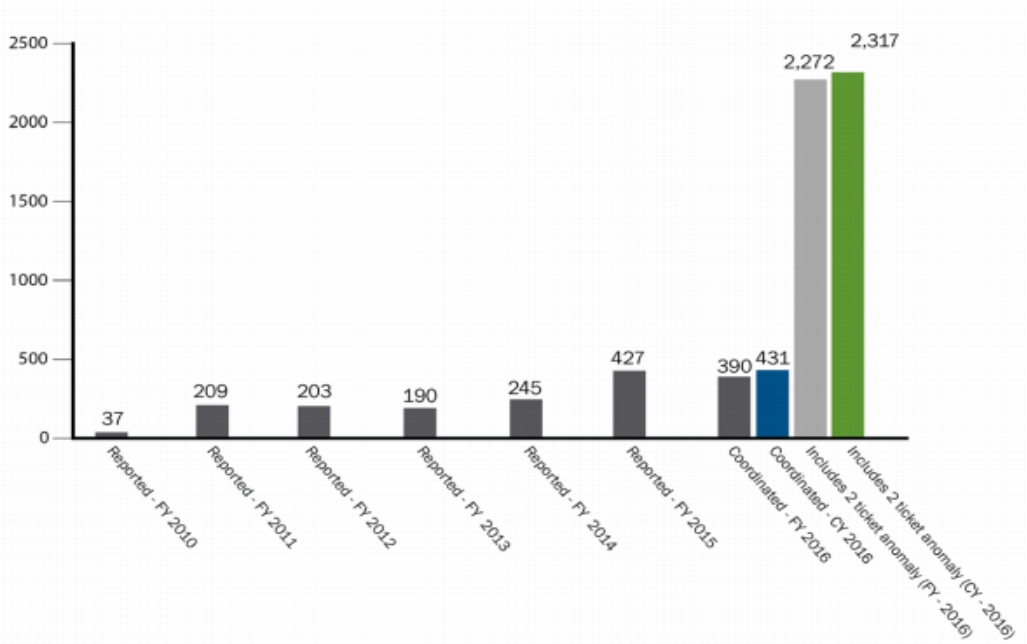
Ref. : Information Security Forum Forecasts : 2019 Global Security Threatt Outlook

Guidelines for Updating Anti-virus Program on OT System onboard of Ships

● How to update anti-virus program on ship`s OT Systems?

Even though there is a lot of debate about the need for anti-virus vaccines due to attacks using zero-day vulnerabilities and various malicious code variants, the fact that vaccines are the basic safeguards for cyber security remains the same. However, unlike information systems such as PCs and servers, vaccine operations are limited in OT (Operating Technology) used in ships. The main reason for this is the fact that the vaccine is not needed yet or management difficulty is the biggest reason. Typically, a software(SW) development company regularly releases security patches to protect SW users. Zero-day attacks are attacks that occur when a company does not recognize a security vulnerability of a particular SW or when a company does not have an official security patch.

Although less well known than information systems, OT security vulnerabilities have been steadily emerging, especially since 2016. The graph below shows that the number of vulnerabilities in 2016 has increased sharply in 2017 as a result of the US ICS-CERT's vulnerability report. It seems clear that the SW vulnerability will continue to be the focus of OT security and the need to operate such measures as vaccines or security patches.



[Status of vulnerabilities reported by ICS-CERT since 2010]

Ref. : Recommended Practice: Updating Antivirus in an Industrial Control System

However, from the perspective of managing the OT system, it is not advisable to unconditionally update the vaccine or apply a security patch. This is because, in the case of an OT system where availability is most important, an error during installation and update (security patch) of a vaccine, a conflict with other system functions, and an issue due to use of an old SW version may occur. This is also the biggest concern for ship management companies. In response, ICS-CERT provided recommendations for the installation and enforcement of the following vaccine updates in August 2018:

- Verify the source of the update. Download the update files to a dedicated host (server)
- Scan the downloaded file(s) for malware : (https://www.virustotal.com)
- Verify the cryptographic hash of each downloaded file(s).
- Scan the removable media for malware or other unexpected data before use to verify its integrity.
- Lock the media so others cannot write to it.
- Load the media into the test environment and verify that it has no adverse impact to the test system.
- Install the update on a non-critical endpoint or segment of the system and verify that it has no adverse impact to the system.
- Monitor the system for any unusual behavior and verify proper operation of the OT

These update procedures may differ slightly depending on the environment and ship of the ship management company. However, the key point is that the integrity of the files received from the outside are maintained, the malicious codes are infected during the process of moving the files, Is the ongoing management of issues. The cyber security of the ship is an important factor that directly affects the safety of the ship. Therefore, it is necessary to establish and operate a systematic procedure rather than a simple update.

▪ This article was written by Jae-woo Im, director at Seedgen co., Ltd.

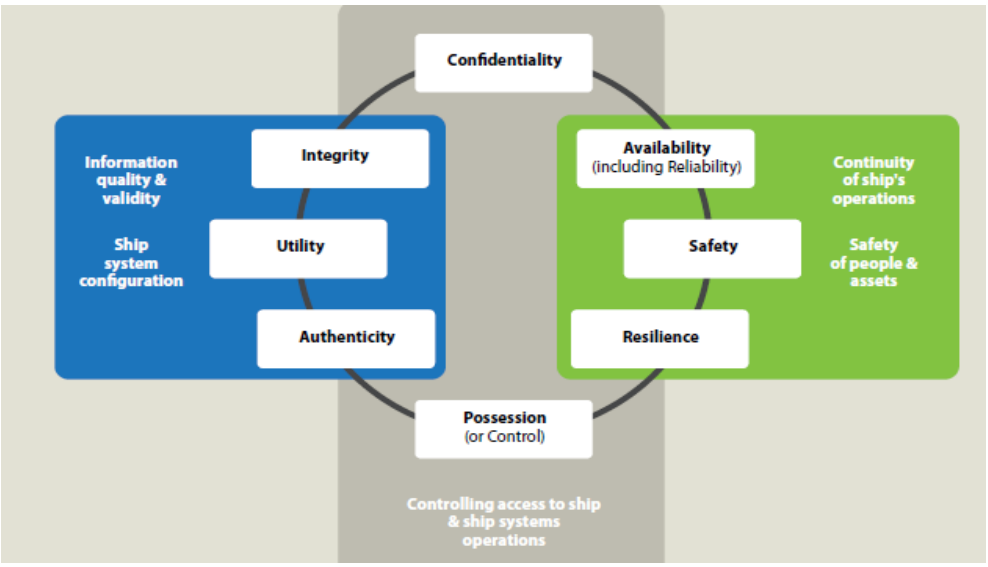
Seedgen is a information security company that provides information security consulting and information security education services. It conducted consulting on ISO 27001 and information protection to 400 companies in the Korean public and industry sectors and provided practical services such as training to enhance awareness of information protection, on- and off-line education, and simulation training.

Cybersecurity Issues and Countermeasures for OT system onboard of Ships

● What is the role of the cyber security officer in ICS/SCADA area?

ICS/SCADA security in the operation zone (OZ) on ships is considered as a separate operating environment from the Internet environment like one of other critical infrastructure, so most workers in maritime industries do not think it is a big consideration for their ships.

To discuss ICS/SCADA security, an understanding of the industrial control systems used throughout the critical infrastructure as well as ships and ports should precede. ICS/SCADA is an acronym for Industrial Control System (ICS) and Supervisory Control And Data Acquisition (SCADA), SCADA is a software that centrally monitors and controls the production process of several plants that are physically separated from each other, and analyzes the system's information from a central location. SCADA can be seen as a system that controls facilities by centrally monitoring and analyzing information collected from PLCs and sensors in unmanned locations through software that controls production processes of many plants that are physically separated. On land, it is used for critical infrastructure networks such as electrical wiring, wastewater treatment system, and subway management system. For ships, GICOMS, AIS, LRIT, and SSASs can be seen extensively within the ICS/SCADA and ship data can be viewed in real time from land using the latest popular mobile applications.



Ref. : IET Standard : Code of Practice Cyber Security for Ships

In fact, there was no need to worry about cyber threats before the ICS was connected to the network, and it was not an issue due to the limited network connection, transmission speed, and transmission capacity of the ship. However OT has steadily developed convergence with IT. Although IT is used for OT, IT staff are being held responsible for cyber security without fully understanding various operational requirements for ship networks. Shipping company already requires the safety and quality management team to play a role in cyber security as an ICS operator.

Then, what should cyber security officer do in the ICS/SCADA area? To reduce the likelihood of cyber attacks to ICS and to quickly recover from attacks, continuous monitoring and log management through vulnerability assessment are required.

- **Vulnerability assessment :** Fixing known vulnerabilities is essential to ICS security. ICS operators should be able to identify vulnerabilities disclosed by major vendors such as Siemens, ABB, Honeywell, and ICS-CERT, and to analyze vulnerabilities disclosed by cyber security-related vendors or organizations.
- **Continuous monitoring :** It is difficult to always identify what is happening on devices such as switches, routers, and firewalls. Furthermore, it is more difficult for network-connected equipment such as servers, workstations, Intelligent Ethernet devices, and PLCs running SCADA. Continuous monitoring is to retrieve all changes occurring in ICS according to security policy by using Security Configuration Management (SCM).
- **Log management :** Various devices of ICS can send logs that contain information about security events such as how the network operates, potential errors associated with outages, and a number of failed logins. Log management is the function to collect logs from various assets such as servers, applications, network devices, firewalls, and databases into a central repository and make them available for forensics analysis.

▪ **This article was written by Seung-jun Lee, senior researcher at NSHC & Shield Consulting co., Ltd**

NSHC SECURITY, the only cyber security company in Domestic and Asian that can carry out penetration testing of ICS/SCADA(OT), is conducting malicious code analysis such as ransomware and APT attacks, penetration testing of industrial devices and source code diagnosis. SHIELD CONSULTING is providing consulting on physical security(CCTV, control of outsider's access, control of electronic devices and locks) required in cyber security.

Understanding of Cyber Threat

● Understanding of 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 November, we will analyze the **"Compromising of Extranet and Cloud Components"** 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 : Compromising of Extranet and Cloud Components

The trend common in conventional IT to outsource IT components is now also gaining traction in the ICS sector. This usually does not concern components directly controlling actual processes. However, the number of providers of externally operated software components in the area of data capture and processing on historians, for the calculation of complex models for the configuration of machines or the optimization of manufacturing processes (Big Data) has been continually increasing. Security specific components are also occasionally offered as a cloud-based solution. For example, providers of remote maintenance solutions place the client systems for remote access in the cloud which the maintenance technicians can use to access the different components.

< Potential threat scenarios >

▣ Interference with or disruption of communication between local production and the outsourced (cloud) components. Cascade effects can also impair local production.

▣ Exploitation of implementation errors or insufficient security mechanisms in order to gain access to data stored externally (data theft, deletion).

▣ If a cloud provider's clients are insufficiently separated, attacks on other cloud services may lead to interferences (collateral damage).

< Countermeasures >

- Contractual obligation of operators of external components to provide a sufficient level, e. g. through a service-level-agreement (SLA).
- Use of trusted and, if possible, certified service providers.
- Operation of a private cloud to retain control and protect process know-how.
- Use of sufficiently strong crytographic mechanisms (encryption, integrity protection) to protect the data stored in the cloud.
- Use of Virtual Private Networks (VPN) to secure the connection between local production and external components.

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

Guidelines of Establishing Access Control Policy

● The need for establishing access control policy

Unauthorized access to the network and files can easily leak company confidential information, so it is necessary to establish appropriate access control policies. The policy should define the tasks that require access control, document how and scope of access control for this task, and define them so that access control targets for data, programs, major systems, networks, etc. can be clearly identified. For security-critical access control rules, only administrative approval should be set up or changed, review and approve the appropriate approach control policy for changes in the surrounding environment, business content, or changes in the information system environment, and regularly monitor and approve monitoring user access rights.

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

Establishing Access Control Policies(206.1) : Access control policies should be established, including standards, principles, and procedures for operating system access rights.

Permissions by user(206.3) : The privileges of the general user and the administrator should be differentiated and the authority standard for each task should be defined.

● Definition of access authority (example)

Classification	Description	Subject
Super administrator	Administrator who have read, write, and execute permissions for all account management, data retrieval and deletion of system or service, and setting of access rights	System administrator
Intermediate administrator	Administrators who have read and write access to the system or service account	Relevant department administrator
User	Users who are authorized by the intermediate administrator and who have the authority to read, write and download data	Person in charge of carrying out business through system
Special authority administrator	System maintenance for the system or service administrator responsible for the vendor, developer, etc. authorized for system operation management	Maintenance agent

● **Access authority criteria (example)**

Asset classification	Access authority type			
	Super administrator	Intermediate administrator	User	Special authority administrator
Network equipment	○	○	-	△
System Server	○	○	-	○
Application	○	○	○	○
Database	○	○	-	○

● **Security System list for access control (example)**

Security system for access control	Location
Firewall/UTM/IPS (Intrusion Prevention System)	Network
ACL (Access Control Layer)	Network
DB access control	System or Network or Application
System access control (Secure OS)	System

※ Security system for each system may be different depending on the application location

● **Checklist Format for access control (example)**

System		Scope	
Inspection Date		Inspector	
Checklist		Result	Remark
1. Access authority termination			
2. Permission changes reflected			
3. Special authority changes or termination			
4. Access authority history record (grant, change, terminate)			

Explanation of Term

- **Global Maritime Forum :** The Global Maritime Forum is a non-profit international organization committed to promoting the potential of the global marine industry. Policy makers, experts, NGOs and other influential marine community leaders to work together to discuss collective tasks and develop new solutions and action recommendations. The annual summit was held in Hong Kong on October 3, 2018.
- **DoS(Denial of Service) :** prevents legitimate and authorised users from accessing information, usually by flooding a network with data. A distributed denial of service (DDoS) attack takes control of multiple computers and/or servers to implement a DoS attack. [BIMCO]
- **VPN(Virtual Private Network) :** enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network, thereby benefiting from the functionality, security and management policies of the private network. [BIMCO]
- **ICS-CERT :** The Department of Homeland Security (DHS) established the US-CERT in September 2003 to protect the U.S. Internet infrastructure for cyberattacks. The National Cybersecurity and Communication Integration Center (NCCIC) was established in 2009 and the US-CERT is affiliated with NCCIC and is working with the Industrial Control Systems Cyber Emergency Readiness Team (ICS-CERT).
- **Cloud :** A technology that stores software and data in a centralized database connected to the Internet so that data is available anywhere, anytime, by simply accessing the Internet. Cloud services leave a security vulnerability to the existing Web environment, requiring cloud security to protect data stored from theft, leakage, and deletions.