KR Cyber Security

News from KOREAN REGISTER

June 2018

Vol. 002

KR Cyber Security Activity

- **Korean Register signs a cyber security MOU with T1**

On May 18, Korean Register of Shipping (KR) and T1 INFORMATION TECHNOLOGY CO., LTD. (T1) signed an MOU to strengthen the mutual exchange of technology and cooperation on joint cyber security research and development between the two organizations. T1 provides high-quality IT services for the marine, communication and shipbuilding sectors and clients such as Hyundai Merchant Marine, HYUNDAI GLOVIS and KTSAT.

The technical cooperation between KR and T1 will include the following:

- Cyber security certification technology cooperation for ship maintenance companies
- Construction of practical training materials for use ashore and on-board
- Technical cooperation for on-board cyber security

It is expected that KR will expand its cyber security certification area as a result of the MOU. Cyber risk assessment technology will be enhanced through the cyber vulnerability analysis and cyber attack analysis of actual IT systems installed on ships. The analyzed data will be incorporated into KR's academy education materials from August.

Increasing reliance on IT is going to mean increasingly big risk

The EU Network Information Security (NIS) directive, which was established by ENISA in May 2016, is expected to affect the shipping system in the long term.

- **EU NIS Directive, Focus on Interactions between freight handling companies and ports**

NIS Directive is a guideline that calls for increased security levels in response to cyber attacks that could compromise transportation, power, transport, financial market infrastructure, medical and digital infrastructure. The minimum requirements of service operators and digital service providers.

- **Increasing reliance on IT = Increasing big risk**

Some shippers and shipping companies have expressed deep concerns in whether this directive applies to systems on board ships as to GDPR. However, Philip Roche, chairman of European Union's Heritage Cyber Risk Management Summit, said the directive will be will be to tighten cyber security at ports including around interactions between freight handling companies and ports, while maritime cybersecurity will continue to be the domain IMO policy and flag states regulation. The move to strengthen the security level of ports and logistics systems will also have a significant impact on the industrial competitiveness of ship operations and cargo management, which are highly dependent on IT.

Response and Suggestion

The EU NIS directive will not affect the ship owners and shipping companies in the near term. In the long run, monitoring of cybersecurity activities, such as in each continent or region, and businesses, is needed to keep up with the competition for cyber security-related compliance. It is necessary to have a better understanding of KR maritime cyber security guides or EU NIS guidelines..

Ref. : Cyber changes : the NIS Directive and the role of tech in transforming shipping, Marine Electronic & Communications, May, 2018

2018 Critical Infrastructure Attack Trend

Cyber attacks on national infrastructure, such as logistic, medical, manufacturing, energy and transport, as well as power networks are expected to continue in 2018.

- **Not considering an Internet connection ICS**

Although cyber security of infrastructure was not considered important until a few years ago, control systems were also found to be no exception to cyber attacks by Iran's Stuxnet, Ukraine's electric power company hacking in 2015, and Maersk' ransomware infection. This problems come from the fact that while ICS devices used in control systems are currently connecting to Internet connections, the initial design of the device did not take these issues into account at all.

- **Supply Chain Threat & Security**

The cybersecurity levels of company-related services and equipment suppliers are as important as the level of hardware and software security. For example The level of cybersecurity of the supply chain or partner workforce that was not monitored or managed as there was no threat of unauthorized access to the network or system by the operator (or cleaner) who knew the system well.

Response and Suggestion

As it is expected that most of phishing attacks will continue to be high in 2018, employees and their partners staffs will need to train and train to increase awareness of cyber security. In addition, from an infrastructure security perspective, access control technologies should be applied to networks that communicate externally and the requirements of cybersecurity should be checked and managed by partner companies. In particular, a HW/SW security review is required for new and legacy assets.

Ref. : Critical infrastructure attacks on the rise, welivesecurity. May, 2018

Cybersecurity, A key factor to the Growth of Maritime Information

Technavio, a market analyst for the technology sector, predicts that the global market information market will grow at least 10 percent annually by 2022.

- **Growth of Communication, Navigation, and to Monitor and Control ships**

The report, which divides the maritime information market into platforms(On-Aru, Vessel), Tracking Technology (AIS, SAR, LRIT), applications, end users, and Region, predicts the growth of the marine industry centered on maritime transport sector. In particular, maritime IT sectors, such as maritime information analysis technology, vessel tracking, and automatic certification system, analyze that the development of the fourth industry combined with the increase of marine trade could save financial human resources. And The development of technology is expected to create a virtuous cycle that will increase trade activities by expanding the opportunity for maritime transport.

- **Key Factor, Cyber Security**

However The report stressed that cybersecurity is the key to advancing digitalization in the maritime sector. Communication, navigation, and ship monitoring and control technologies, which are representative information technologies that are applied to ships in recent years, require cybersecurity.

Response and Suggestion

Information technology is being introduced to reduce costs and efficiently deploy resources, and maritime areas can not be excluded. However, a reliance on IT should be based on cybersecurity, and ship operating companies and others should be careful not to disrupt productivity by applying cybersecurity security review and development security of SW development materials when IT resources are introduced.

Ref. : Global Maritime Information Market Analysis 2018 Forecast to 2022 with Inmarsat, Business Wire, May, 2018

Guideline for Cyber Security Organizations

- **The need for cyber security organization guidelines**

In order to respond to increasing cyber security threats and to maintain and enhance an organization's cyber security levels, it is necessary to define the responsibilities and roles for managing cyber security activities. Company`s cybersecurity organization guidelines identify the functions, structure, roles, and designation of key tasks necessary for the effective development of a cyber security organization.

- **Cyber security organization and role and responsibility**

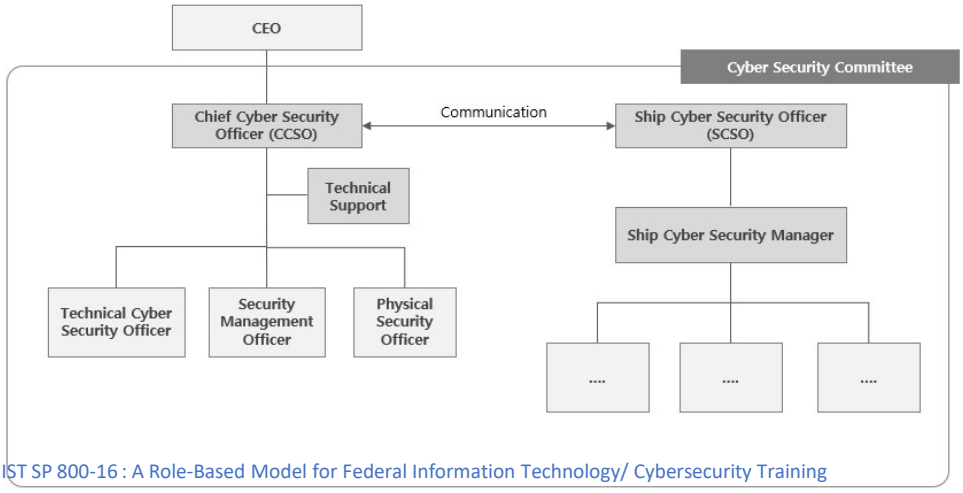
1) Chief Cyber Security Officer (CCSO)
This refers to a person who manages overall security related business including cyber security, establishment of security policy, organization of security, risk management (NIST Standard : CIO)

2) Technical Cyber Security Officer
The person who establishes policies covering the technical aspects of the company's cyber security, especially cybersecurity risk analysis and assessment, implementation of countermeasures, cybersecurity incident response and recovery, training management.

3) Security Management Officer
The person who establishes the security management procedures and planning for the company, carrying out periodic verification to improve the security system including cyber security.

4) Physical Security Officer
The person who is responsible for planning and implementing the cybersecurity physical parts for physical risks, such as coordinating the execution and planning of the cybersecurity physical parts

5) Ship Cyber Security Officer(SCSO)
The person who is responsible for the organization, operation and activities of cybersecurity organizations in ships, coordinating issues of cybersecurity activities between ships and companies, improving the security.



Ref. : NIST SP 800-16 : A Role-Based Model for Federal Information Technology/ Cybersecurity Training

Explanation of term

- **NIS Directive** : 'The Directive on security of network and information systems' is a cyber security guideline that was established in May 2016 based on ENISA(European Union Agency for Network and Information Security), an organization under EU Cyber Security. It specifies what system operating bodies such as businesses and government agencies should do for cybersecurity. However, unlike the EU GDPR, it is not mandatory to comply at the level of non-law guidelines.
- **GDPR(General Data Protection Regulation) :** EU Data and Privacy Act. It is known that more than 98% companies that are carried out within EU territory that have been implemented since May 2018 are applied to relevant laws and focuses on guaranteeing rights of information entities that provide personal information. From the first day of entry into force of the law on May 25, large IT companies such as Facebook and Google were sued for violating the GDPR, while major U.S. media service companies suspended access to the homepage from the EU to avoid the lawsuit.
- **Supply Chain Security** : Supply Chain security refers called Supply Chain Management, as a result of a series of management processes that look at logistics flows from a supplier of components to a producer to a distributor to a customer from a single value chain perspective. This means that some of the various companies in the Supply Chain's range of cyber security threats could emerge as a threat to the entire chain.
- **Phishing Attack :** One of social engineering attacks. It is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication