KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 015

July 2019

KR Cyber security Activities

- KR awards cyber security AIP certificate to Yokogawa Electric co. Korea
- KR delivers customized cyber security trainging for Sansho co. Korea
- Maritime Cyber Risk Management Forum 2019

IMO MSC 101th, Result of discussion for cyber security

Understanding cyber threats(OWASP Top 10)

Guidelines for establishing cyber security internal audit

Explanation of Term

KR Cyber security Activities #1

KR awards cyber security AIP certificate to Yokogawa Electric co. Korea

The Korean Register of Shipping (KR) presented a Certificate of Approval in Principle (AIP) to the Integrated Automation System (IAS) of Yokogawa Electric Co., Ltd. Korea on 5 July 2019.

KR's Cyber Security AIP is a process that approves the basic design of a cyber safety system which offers comprehensive protection against cyber threat, an increasingly important topic for the shipbuilding industry.

Yokogawa Electric's integrated automation system (IAS) is a system primarily designed for LNG carriers. It controls and monitors the cargo system and the mechanical system, as well as the LNG boil-off gas (BOG) management system. KR evaluated the basic concepts based on IEC 62443, the international standard for cyber security and the NIST standard, and following detailed analysis awarded the AIP certificate to Yokogawa Electric's IAS system. Cyber security risk management will be a priority for the International Maritime Organization (IMO) from 2021, and as a result the demand for cyber security type approval of systems onboard ships is expected to increase.

KR has developed a cyber security type approval service based on international standards IEC 62443 and IEC 61162-460. KR's technical review covers confidentiality, integrity, availability and recovery function as the basic requirements of any cyber security system as part of the cyber security authentication service.

KR Cyber security Activities #2

KR delivers customized cyber security training for Sansho co. Korea

On July 9, KR delivered customized training on cyber security for OCIMF TMSA for Sansho kaiun Co., Ltd. following the company's OCIMF TMSA inspection in May, 2019. The participants from Sansho co. expressed their gratitude to KR for the training, with representative Mr. Lee ho-gil requesting a follow up business seminar for overseas crew members. KR received favorable feedback from Songa Ship management located in Glasgow, Scotland following its TMSA inspection in April, 2018, which was also prepared for by conducting pre-audit of cyber security. Moving forward, KR plans to strengthen its customized training on cyber security tailored to the needs of ship owners, shipyards, and equipment manufacturers.

OCIMF TSMA(3rd)	OCIMF SIRE VIQ (7th)
13.1.2 The company has documented procedures in place to identify security threats applicable to vessels trading areas and shore-based locations.	7.14 Are Cyber Security Policy and Procedures part of the Safety Management System and is there a Cyber Response Plan onboard?
13.2.3 Policy and procedures include cyber security and provide appropriate guidance and mitigation measures.	7.15 Are the crew aware of the company policy on the control of physical access to all shipboard IT/OT systems?
13.2.4 The company actively promotes cyber security awareness.	7.16 Does the company have a policy or guidance on the use of personal devices onboard?
13.3.2 Security procedures are updated taking into account current guidance.	7.17 Is Cyber Security awareness actively promoted by the company and onboard?
13.4.5 The company is involved in the testing and implementation of innovative security technology and systems.	

KR Cyber security Activities #3

Maritime Cyber Risk Management Forum 2019

KR attended the Maritime Cyber Risk Management Forum 2019 held in London, UK on 25 June, for an update on the latest developments in international trends and technologies.

The forum consisted of six sessions on different topics which were actively discussed by maritime industry experts. There were presentations on the rules and regulations for cyber risk management, the viewpoints of ship owners and operators, cyber security accident training, port cyber security threats, countermeasures against maritime cyber attacks. The discussions confirmed that the maritime industry needs to prepare strong cyber security responses and adopt a robust strategy. Session 2 examined recent cases of cyber attack (ransomware) in June 2017 with presenter Andy Powell (Chief Information Officer of CISO) of Musk Shipping, discussing the five core operating principles (responsibility, risk management, trust, resilience, and cyber security benefits).

In order to build an effective maritime cyber security response system, it is essential to first clearly identify the responsibilities and roles of various stakeholders in the maritime industry (ports, ship owners, ships, shipyards, manufacturers, service companies, etc).

SESSION	PROGRAMME
[Session 1] REGULATIONS, COMPLIANCE AND RISK MANAGEMENT	· Legal and regulatory compliance in the cyber incident response context · The guidelines on cyber security onboard ships · Insurance cover for liability and property damage arising from a cyber incident
[Session 2] A VIEW FROM SHIPOWNERS AND SHIP OPERATORS	· Vendor Risk Management · Implementing the lessons learned from a major cyber attack · Cyber lessons learned from Industrial Control Systems
[Session 3] CYBERSECURITY INCIDENT SIMULATION EXERCISE	· What is the magnitude of cyber risk?
[Session 4] THREATS TO CYBERSECURITY IN PORTS	· Innovative Risk and Security Management solutions for protecting European Ports and their Supply Chains · Resilience planning - Maritime ports to up their game in cybersecurity · Using AI for Real-Time Threat Detection across OT & IT
[Session 5] HOW TO PREVENT CYBER-ATTACKS FROM HAPPENING?	· The weakest link: the role of human error in cybersecurity
[Session 6] CYBER SECURITY HUB	· Challenges in maritime incident response · The CIRM Cyber Risk Code of Practice for Providers of Marine Electronic Equipment and Services

Source : https://www.shipcybersecurity.com/index.htm

IMO MSC 101th, Result of discussion for cyber security

MSC 101 at IMO, next steps for maritime cyber risk management

The International Maritime Organization's (IMO) 101st Maritime Safety Council (MSC) meeting held in June 2019 at the IMO headquarters in the UK, discussed maritime cyber risk management. In particular, this meeting raised the need for integrated management of maritime cyber risk that satisfies both ISM and ISPS requirements. The IMO adopted resolution MSC.428 (98) to include cyber risk in the ship safety management system (SMS) of the ISM Code at its 98th MSC meeting in July 2017, It encourages compliance with the DOC's (documentation of compliance) first annual review. However, there is a concern that the contents of the two documents may not coincide with each other due to the separate Safety Management System (SMS) of the ISM code and the ship security plan (SSP) of the ISPS code. In the case of the SSP, the administrative burden increases for shipping companies because it needs to be approved by the government whenever it is changed. Therefore, in order to solve this problem, the IMO will deal with physical security matters in the SSP according to the ISPS codes, but if there is a cybersecurity management system in the SMS, it will come under a separate risk management system. This decision was made at the 101st MSC meeting, and serves to ensure that the Cyber Risk Management System is secured for the DOC and SMC (safety management certificate) after January 1, 2021, when the ISM Code becomes effective pursuant to IMO Resolution MSC.428 (98) (SSP) and is only intended to refer to the cyber risk management procedures found in the SMS of the ISM Code.

IMO included cyber risk management in MASS guideline

At this IMO MSC meeting, a draft for marine commissioning guidelines for the pilot operation of Maritime Autonomous Surface Ships (MASS), was prepared to include measures for the management of maritime cyber risk.

The draft guidance reflects the system and infrastructure used to conduct self-propelled ship testing, while ensuring adequate cyber risk management. As a result, it will be necessary to consider cyber security from the initial stages of policy development and technical standard development, particularly for the smart port and autonomous operation vessels which are expected to be promoted in the future.

Understanding cyber threats(OWASP Top 10)

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

The Open Web Application Security Project (OWASP) is an open source web application security project, researching web exposure, malicious files and scripts, and security vulnerabilities. The OWASP Top 10, which is frequently referred to, highlights the top web application vulnerabilities, it was published in 2004, 2007 , 2010, 2013 and 2017. In this newsletter we will analyze the **'A6 : 2017 – Security Misconfiguration'**

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

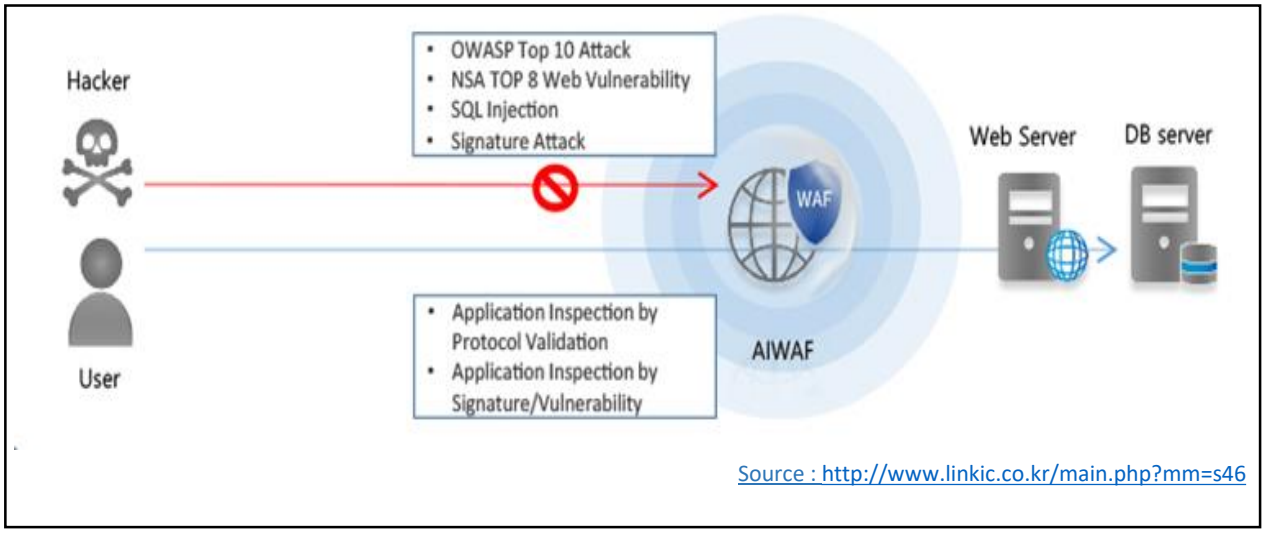
Source : OWASP Top 10 Project

OWASP Top 10 'A6 : 2017 -Security Misconfiguration'

Security Misconfigurations are the most common issues that result from poorly configured defaults, incomplete (or temporary settings), open cloud storage, misconfigured HTTP headers, and verbose error messages that contain sensitive information. All operating systems, frameworks, libraries and apps must be securely configured.

<Response Policy>

- **URL extension access control** : Define extensions requested from client
- **Default page access detection** : Administrator page access detection
- **Directory Listing** : Preventing the file information by wrong setting of the web server
- **Error page clocking** : Check the response code of the web server and send the phrase specified by the administrator



Source : http://www.linkic.co.kr/main.php?mm=s46

Is the Application Vulnerable?

The application might be vulnerable if the application is:

- Missing appropriate security hardening across any part of the application stack, or improperly configured permissions on cloud services.
- Unnecessary features are enabled or installed (e.g. unnecessary ports, services, pages, accounts, or privileges).
- Default accounts and their passwords still enabled and unchanged.
- Error handling reveals stack traces or other overly informative error messages to users.
- For upgraded systems, latest security features are disabled or not configured securely.
- The security settings in the application servers, application frameworks (e.g. Struts, Spring, ASP.NET), libraries, databases, etc. not set to secure values.
- The server does not send security headers or directives or they are not set to secure values.
- The software is out of date or vulnerable (see A9:2017-Using Components with Known Vulnerabilities).

Without a concerted, repeatable application security configuration process, systems are at a higher risk.

How to Prevent

Secure installation processes should be implemented, including:

- A repeatable hardening process that makes it fast and easy to deploy another environment that is properly locked down. Development, QA, and production environments should all be configured identically, with different credentials used in each environment. This process should be automated to minimize the effort required to setup a new secure environment.
- A minimal platform without any unnecessary features, components, documentation, and samples. Remove or do not install unused features and frameworks.
- A task to review and update the configurations appropriate to all security notes, updates and patches as part of the patch management process (see A9:2017-Using Components with Known Vulnerabilities). In particular, review cloud storage permissions (e.g. S3 bucket permissions).
- A segmented application architecture that provides effective, secure separation between components or tenants, with segmentation, containerization, or cloud security groups.
- Sending security directives to clients, e.g. Security Headers.
- An automated process to verify the effectiveness of the configurations and settings in all environments.

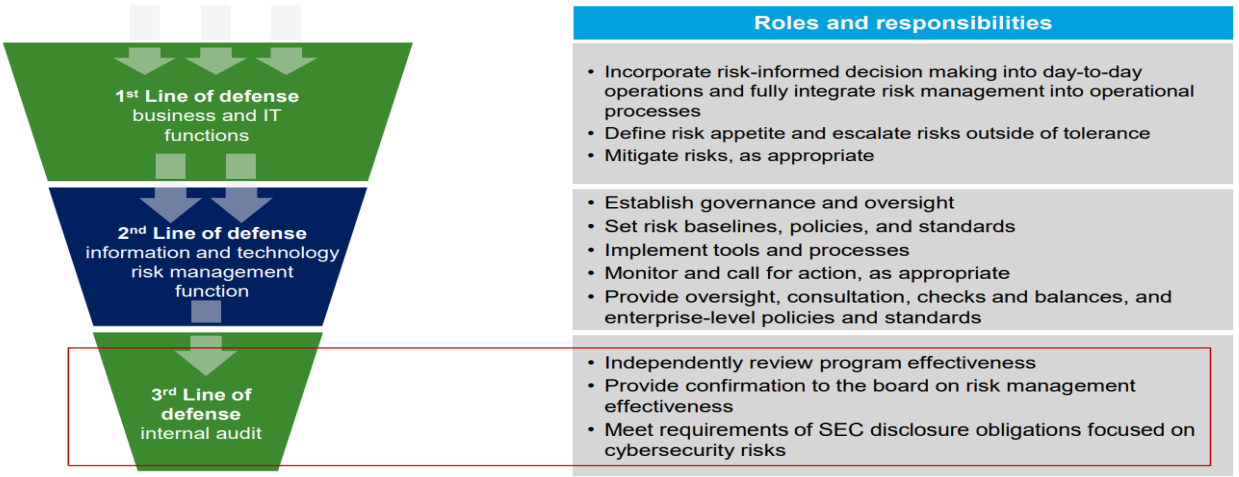
Source : OWASP Top 10 - 2017

Guideline for Cyber security Internal Audit

Definition of Cyber security Internal Audit

The biggest threat to cybersecurity could be internal employees or suppliers. Cyber attacks involving insiders (employees, suppliers, or other companies legitimately linked to the company's computer systems) are deadly and increasing. Such instances now account for more than 20% of all cyber attacks. Conventional safety devices that are widely used are ineffective in preventing this.

To reduce vulnerabilities to insider attacks, companies should make cybersecurity a priority, as much as quality and safety. That is to say, every employee should think of security as part of their work. If suspicious activity is detected, employees should be closely monitored to ensure that they are notified and that they will be informed of the potential threats. Suppliers and distributors are urged to minimize risk and conduct periodic audits and leaders must work closely with their IT departments to protect the company's key assets.



Source : Deloitte, Cybersecurity The role of Internal Audit

KR Guidance for Maritime Cyber Security System requirement (CS1)

Check the actual condition(219.1) : The company should conduct a half-yearly security check.

Report violations(219.2) : Policy violations should be reported in accordance with cyber security internal audit plan.

Checklist for Cyber security Internal Audit

HUMAN SECURITY	Yes	No
1. Do visitors to the company wear security badges?		
2. Do you have a process for effectively cutting off access to facilities and information systems when an employee/ contractor terminates employment?		
3. Do you have policies addressing background checks for employees and contractors?		
4. Has a cyber security training list been established?		
5. Has there been any disciplinary action taken for cyber security breaches?		
PHYSICAL SECURITY	**Yes**	**No**
6. Do policies and procedures specify the methods used to control physical access to your secure areas, such as door locks, access control systems, security officers, or video monitoring?		
7. Is access to the computing area controlled (single point, reception or security)?		
8. Are visitors escorted in and out of controlled areas?		
9. Are your PCs inaccessible to unauthorized users (e.g. located away from public areas)?		
10. Is your computing area and equipment physically secured?		
ACCOUNT AND PASSWORD MANAGEMENT	**Yes**	**No**
11. Do policies and standards cover electronic authentication, authorisation, and access control of personnel and resources to company information systems, applications and data?		
12. Are controls in place to ensure only authorised personnel have access to company computers?		
13. Are controls in place to enforce appropriate passwords?		
14. Are passwords secure (not easy to guess, regularly changed, no use of temporary or default passwords)?		
DISASTER RECOVERY	**Yes**	**No**
15. Is there a business continuity plan?		
16. Is there a process for creating retrievable back up and archival copies of critical information?		
17. Do you have an emergency/incident management communications plan?		
18. Is there a procedure for notifying authorities in the case of a disaster or security incident?		
19. Does the procedure identify who should be contacted, including contact information?		
COMPLIANCE & AUDIT	**Yes**	**No**
20. Are security documents, such as: policies, standards, procedures, and guidelines, reviewed and updated on a regular basis?		
21. Do you audit the processes and procedures for compliance with established policies and standards?		
22. Are employees aware to keep their passwords secure?		
23. Are employees able to identify and protect classified data, including paper documents, removable media, and electronic documents?		
24. Does the awareness and training teach proper methods for managing personal private information?		
25. Do you test your disaster plans on a regular basis?		

Explanation of Term

SQL Injection

Typical WEB hacking technique in which an attacker inserts a statement with malicious intent in addition to a general value between the process of querying the database behind the WEB application and executing the SQL query statement desired by the attacker.

Directory Listing

Vulnerability in vulnerable server configuration causes file storage and browsing to be seen on the web. It can be used for the second and third attacks because it provides the attacker with leakage of account information and various information due to leakage of the backup file, source code, and script file.

Error page Clocking

When a clearance side error and a server side error or a debugging error occur in the web application through the server and the error page setting, unnecessary information such as server setting information and sensitive data can be prevented from being exposed to external users.