KR Maritime Cyber Safety News & Report

Vol. 057
March. 2023

Korean Register
www.krs.co.kr

CONTENTS

KR and SIRM launch cyber security e-learning training

Editor : AHN Jongwoo, Korean Register

< 왼쪽부터 Mr. Emanuele Traversa (BU Manager Value Added Services of SIRM Italia), Mr. Claudio Aleandri (CEO/COO of SIRM Italia), Mr. PARK Joosung (Regional manager / Senior Vice President of KR), Mr. Maurizio Saponara (Project Manager & Business Analyst of SIRM Italia) >

Korean Register (KR) has launched maritime cyber security officer e-learning training in conjunction with maritime technology company SIRM Italia. The training will be delivered to Oltremare, a company in Assarmatori National Shipping Association which provides training to its members.

The new course covers administrative security and cyber risk assessment as well as understanding and practice of maritime cyber security. The course is designed for ship officers who are required to undertake cyber security related audits and surveys.

Hyungchul LEE, KR Chairman & CEO, said: “With so many computer-based systems onboard, ships are vulnerable to cyber risk. Comprehensive cyber security preparedness is now essential for any maritime industry. This e-learning training allows superintendents and crews at all levels to continue their training, to understand and take actions to manage cyber security risk. We will

provide quality training to European customers, starting with providing this cyber security e-learning training to OLTREMARE."

Claudio Aleandri, CEO /COO of SIRM Italia said: "With rapid advancement in technology, shifting cyber threat landscape and increased digitalization, organizations are exposed to greater cybersecurity risks that may potentially have an adverse impact to their business objectives. It is imperative to prioritize and plan defenses to avert those risks effectively. Organizations should be able to identify 'what could go wrong' and determine the levels of cybersecurity risk that they are exposed to, developing adequate assessment and adapting ICT infrastructure. Improving an internal cyber risk awareness culture, through dedicated training, is the strategic approach to protect the organizations and facilitate their governance."

KR has long-established expertise in this area, and developed its cyber security technical and certification services in line with international security standards including ISO 27001, IEC 62443, the NIST Cybersecurity Framework, IMO and BIMCO cyber security guidelines. Also, KR has provided cyber security technical and certification services for companies and ships since 2018, and cyber security type approval services for equipment or system installed on ships in compliance with IEC 62443 4-2 and IEC 61162-460 standards since 2019.

SIRM Italia

SIRM Italia S.r.l. - @hya holding company - is one of the leading companies in the supply, management and maintenance of electronic equipment on board ships (merchant, military and yacht) and in the provision of advanced services for Telecommunications and Digital Transformation of business processes through IT solutions, Cloud and IoT. SIRM Italia is positioned on the market as an independent supplier, thanks to the consolidated relationships with the main producers and international operators in the sector, to always offer the best solution to meet the needs of the customer in relation to the type of ship and operational needs. In this context, another aspect which characterizes the company, is the particular attention shown over the years to the training sector both internally and towards maritime personnel.

KR established Task Forth Team for construction of classification service on ship cyber resilience

Editor : KIM Juntae, Korean Register

The International Classification Society (IACS) issued the Unified Rules (UR) E26 and E27 last year, which are the unified rules for cyber resilience of ships and onboard equipment, and class survey for cyber resilience of new ships contracted for construction on or after 1 January 2024 will be mandatory. In this regard, Korean Register established Task Force Team (TFT) for construction of class survey service for UR E26 and E27 February this year and respond smoothly to inquiries from customers.

The activity period of this TFT is total 11 months from February to December of this year, and the main tasks of the TFT include the development of classification rules in accordance with UR E26 and E27, establishment of new and existing ship inspection processes, and development of type approval services, etc.

By completing the establishment of the cyber resilience inspection service system within this year, Korean Register aims to secure classification inspection capabilities and technology for cyber resilience that will be applied from next year and increase customer service satisfaction through the provision of high-quality technical services.

Cyber attack hits Port of Lisbon

Source : Safety4sea

The Port of Lisbon is under cyberattack, as it reported that criminals are threatening to release confidential port financial information unless their ransom demands are paid.

According to local media, the port authority confirmed that it was attacked on Christmas Day but said that it has been able to continue operations.

Image source: The Maritime Executive

As the port stated to the Portuguese newspaper Publico, “all security protocols and response measures planned for this type of occurrence were quickly activated.”

“The Administration of the Port of Lisbon is working permanently and closely with all the competent authorities, in order to guarantee the security of the systems and respective data”

According to reports, the cyberattack was launched on December 25 taking down the port’s website and internal computer systems. The website remained offline four days later.

Cyber analysts further reported that the attack was staged using a widespread malicious software program called LockBit. The perpetrators posted statements to the “dark web” demanding a ransom of $1.5 million and setting a deadline on January 18 for the payment.

According to the hackers, they managed to capture a broad range of confidential data from the port authority. They are also claiming to possess financial reports, company audits, budgets, contracts, cargo manifests, ship logs, information about crewmembers, personal data of customers, and port documentation, along with other vital Port of Lisbon information.

Source: https://safety4sea.com/cyber-attack-hits-port-of-lisbon/

USCG: New maritime cyber-security assessment

Source : Safety4sea

The US Coast Guard released the Maritime Cybersecurity Assessment & Annex Guide (MCAAG), to help Maritime Transportation Security Act (MTSA)-regulated facilities and other Marine Transportation System (MTS) stakeholders address cyber risks.

This voluntary guide serves as a resource for baseline cybersecurity assessments and plan development, particularly the Facility Security Assessments (FSA) and Facility Security Plans (FSP) required by MTSA.

The MCAAG may be also a resource for Area Maritime Security Committees in assessing overall port area cybersecurity risk and development of cyber annexes of Area Maritime Security Plans and is useful for any other MTS stakeholders interested in conducting a baseline cybersecurity risk assessment, developing plans, as well as the continued improvement of existing plans.

#1 Identify a Cybersecurity Officer

Creating a Cyber Annex requires a thorough understanding of the cyber-enabled systems that affect facility security, the networks those systems are connected to, the cyber threats that affect those systems and networks, and the cyber protections available to the facility.

It is recommended a Cybersecurity Officer (CySO) be identified to provide support to the FSO during the entirety of the Cyber Annex development process. The CySO may be a single person, a group of people, or the FSO. The guidance provided in the MCAAG is intended to aid FSOs in their collaboration with a CySO to produce the Cyber Annex.

Portions of this guide, particularly the technical aspects, assume a CySO with the appropriate cybersecurity experience has been identified and is a part of the Cyber Annex development process.

#2 Determine Scope

Facility security processes and functions are increasingly reliant on computers or computer-

-based systems, such as networked video monitors and electronic badge systems.

Typically, these systems are attached to networks. If these networks are attached to the internet, even in an indirect manner, cyber-attackers can penetrate the facility's networks and subvert the facility's security processes and functions by disabling or altering the systems they rely upon.

When a physical vulnerability involves one or more cyber-enabled systems, there is a challenge in determining the scope of any cybersecurity plan to protect those specific systems.

Most cyberattacks on facilities involve a cyber attacker making an initial entry on a facility network by way of a system that connects to the internet and then moving internally from system to system until they can compromise the targeted system.

Thus, there is a strong argument to be made that any plan to protect a particular system relies on the protection plan for the entirety of the facility's networks.

The recommended approach to determine the scope of the cybersecurity protections contained in the Cyber Annex is as follows:

- Identify all cyber-enabled systems associated with physical security controls or physical vulnerabilities
- Identify the networks these systems attach to. If two networks have a physical network connection between them, consider them to be a single network (even if there are robust boundary protections such as firewalls between them). Note, for many facilities, there will be only one network
- When describing cybersecurity protections to remediate vulnerabilities, describe the plan to protect the network the associated systems operate on

#3 Establish Cybersecurity Vulnerability Definition

It is strongly recommended that the FSO and CySO establish and agree upon an approach to define and identify cybersecurity vulnerabilities in the context of the FSA and that this approach is reviewed and endorsed by the facility's senior leadership and relevant risk managers.

It is recommended that the facility have a formal risk management process by which senior leaders and risk managers can describe acceptable and unacceptable levels of risk and through which the definition of FSA-related cybersecurity vulnerabilities can be determined.

Two observations may be helpful:

- NVIC 01-20 asserts that "It is up to each facility to determine how to identify, assess, and address the vulnerabilities of their computer systems and networks."
- "Cybersecurity vulnerability" is a flexible concept that can be understood at the programmatic and policy level, the system design and configuration level, and all the way down to the level of individual exploitable software flaws in an operating system or application.

To create a Cyber Annex to support an FSP, it is recommended that cybersecurity vulnerability be defined at the program and policy levels, not at the individual system configuration or patch level. For example, if one or more systems critical to the security of the facility are not correctly patched, then possible vulnerabilities to address in the Cyber Annex might include:

- The facility does not have a defined patching policy
- The facility does not have defined patching procedures and/or assigned personnel
- The facility's patching procedures are not fully implemented

#4 Determine the Cybersecurity Vulnerabilities for the FSA

After the FSO and CySO have determined how to define cybersecurity, effective identification of vulnerabilities can be done in three steps:

- Step 4(a): Assemble a team of subject matter experts with adequate knowledge of the facility's physical security, IT, OT, and cybersecurity operations
- Step 4(b): Collect sufficient organizational information to ensure the cybersecurity vulnerability assessment team has adequate visibility and awareness
- Step 4(c): Collaboratively compile a list of cybersecurity vulnerabilities and crossreference them to the physical security vulnerabilities in the FSA

#5 Create Remediation Plans

Each vulnerability addressed in the Cyber Annex should be accompanied by a plan to remediate it. In the same way, it is recommended to describe vulnerabilities at the programmatic, policy, and procedure levels, it is recommended protections be articulated at the same level.

For the purpose of the MCAAG, the term cybersecurity protection will be defined as a discrete unit of a facility's cybersecurity protection plan12. Examples of cybersecurity protections include, but are not limited to cybersecurity:

- Program capabilities
- Policies
- Procedures

#6 Create the Cyber Annex

The recommended Cyber Annex template is structured as follows:

- List the physical security vulnerabilities from the FSA and FSP with identifiers;
- List the cybersecurity vulnerabilities to be addressed in the Cyber Annex with identifiers;
- List the cybersecurity protections that will collectively address the identified cybersecurity vulnerabilities.

Source: https://safety4sea.com/uscg-new-maritime-cyber-security-assessment/

Cloud industry status and security issues

Source : Son Hyun Gu, IGLOO Corp.
Editor : SON Gumjun, Korean Register

Overview

As Corporate infrastructure and data move from o-premises to cloud, a wind of change has come to the cloud market, such as convergence and integration of on-premises and cloud services, or hybrid cloud that combines multiple public clouds, and multi-cloud.

The most important environmental, social and governance(ESG) task in the information technology(IT) the unprecedented spread of COVID-19, a thorough security strategy and countermeasures are required to safely use cloud services as companies and government agencies increase cloud adoption as they rapidly transition to a non-face-to-face society.

In this issue, we will compare and analyze the rapidly changing Korea and oversea cloud markets to examine the future development direction and identify key issues to be considered in cloud security according to the changes.

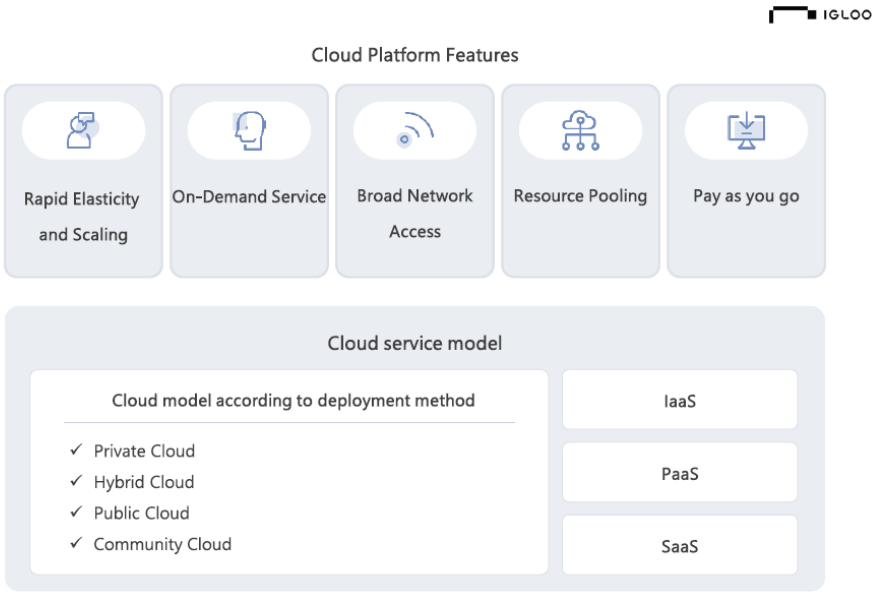


그림 1. Cloud service features and models

(참고: NIST(National Institute of Standards and Technology, US National Institute of Standards and Technology) – Definition of Cloud Computing

Korea and overseas cloud market status

The cloud service model is largely divided into three SaaS(software as a service), laaS(infrastructure as a service), and PaaS(platform as a service). Typically, SaaS is Salesforce, laaS is Amazon(AWS) and Google Cloud, and PaaS is Microsoft(Azure). As Korean cloud companies, KT and Naver are continuously increasing their market share.

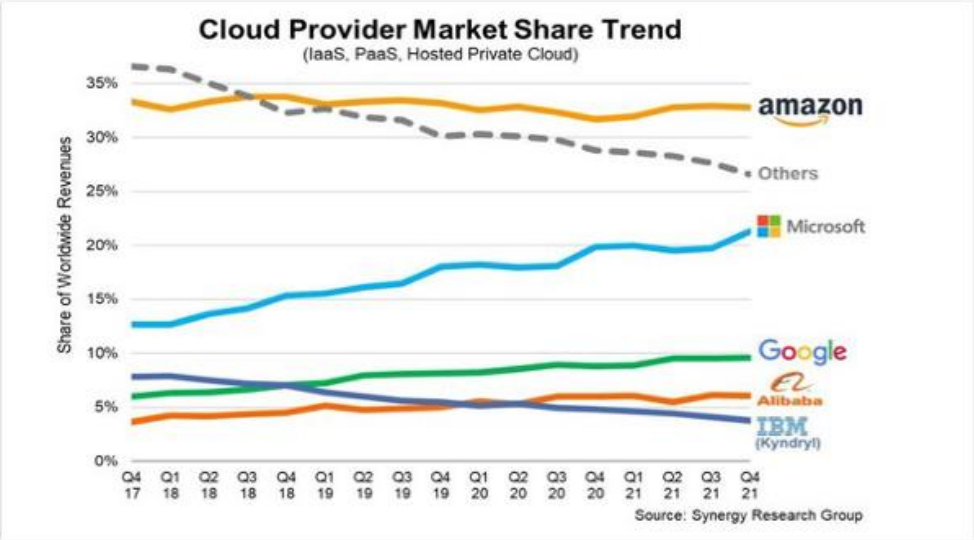


Figure 2. Share of Cloud Companies in 2021 (source : Synergy Research Group)

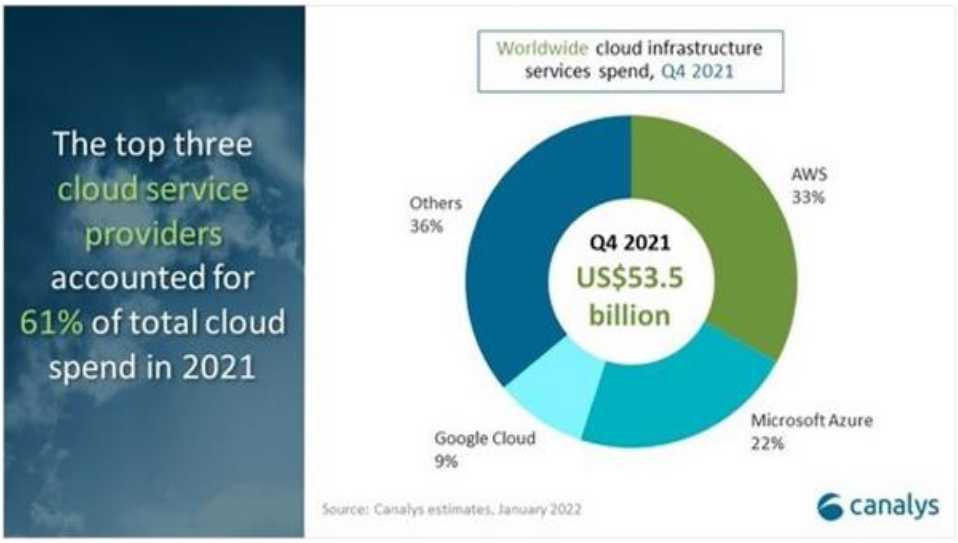


Figure 3. Cloud market share in Q4 2021 (source : canalys)

1) Korea cloud market

As the cloud transition of various organizations such as finance, public service, and education continues to accelerate after COVID-19, the IT infrastructure introduced into the cloud environment is expected to exceed 50% of the total market in the future.

Korean companies are growing by expanding the demand for SaaS, which provides services on a pay-as-you-go basis and subscription cost-based infrastructure-services.

Cloud transition in the public sector is in its infancy and there is a limit to the spread of cloud across the country due to lack of institutional and financial support.

When the government lays the foundation for industry development with the enactment of the Cloud Computing Act('15.3) to create and environment for using the cloud industry, and financial companies and e-finance companies want to use cloud services with the revision of the Electronic Financial Supervision Regulation('19.1) the "Guideline for the use of cloud computing services in the financial sector" was distributed, which aims to guide the detailed procedures required and to recommend necessary security matters for financial system safety and financial consumer protection, thereby expanding the base of cloud use by financial institutions.

In addition, the '3rd Cloud Computing Basic Plan(2022 ~ 2024)' was decided at the '14th information and Communication Strategy Committee' hosted by the Ministry of Science and ICT. Through this, over the next three years, the goal was to expand 300 digital services for public use, achieve 3,000 Korean cloud-specialized companies, and train 10,000 cloud talents.

In fact, the cloud fever is rising in the Korean financial sector, which has been conservative in digital transformation.

According to a survey conducted by the Financial Supervisory Service on 110 financial companies, including 22 banks and 21 security companies, the adoption of cloud in the financial sector is on the rise. In December 2017 alone, the cloud was applied to 47 systems from 23 companies, and in June 2020, the number increases to 145 systems from 42 companies.

2) Overseas cloud market

With AWS as the main axis, Microsoft and Google are in oligopoly of the cloud service market. IN the midst of global digital transformation, the US and Europe are concurrently implementing cloud activation policies to secure leadership in the data economy.

Overseas companies are already converting and providing their services in the form of cloud.

Using this point, they are growing by expanding the demand for laaS and PaaS to develop their services on the cloud infrastructure foundation.

Hybrid and multi-cloud can take advantage of maintaining legal compliance and maximizing service speed and availability, so they are transitioning to a next-generation integrated cloud service environment.

Nation	Major Content
 US	Change from Cloud First policy to Cloud Smart policy, and reorganize regulations and procurement system for cloud expansion • Concentrate on public service innovation based on high-quality/high-tech services in the private sector, and organizations that require high security (Ministry of Defense, CIA, etc.) use private services according to security regulations ※ US can introduce cloud in all areas if FedRAMP standards are met (including security information such as secrets)
 UK	Promote the public sector cloud distribution and utilization by operating a digital service specialized contract system and providing a market, and promote the 'Public Cloud First' policy ※ The UK informatization budget is twice the size of Korea, and 12,150 SaaS are available in the public sector ※ 38,000 services provided by 5,224 companies through the digital marketplace, transaction performance of £9.49 billion (as of September '20)
 EU	Designate cloud as a key industry ('20) and promote the GAIA-X project to establish a foundation for data production/storage/analysis/processing and sharing/exchange in Europe ※ A project to build a cloud ecosystem in Europe to reduce dependence on global companies such as AWS, Microsoft, and Google and secure data sovereignty
 Australia	Announcing the 'Secure Cloud' strategy (2017) and proposing 7 principles for cloud transformation in the public sector to promote the use of private cloud first ① Approach based on risk analysis when applying cloud security, ② Service design to be suitable for cloud, ③ Public cloud service is basic, ④ Cloud use to the maximum, ⑤ Avoid customization and use the service as it is, ⑥ Make the most of cloud automation technology, ⑦ Monitor service status and usage in real time
 China	Announcing the '14th Five-Year Plan (2021-2025) ('21)', which aims to raise the digital economy core industry to 10% of GDP by 2025, cloud computing as one of the seven key areas for digital transformation selected and actively disseminated

Figure 5. Cloud-related policies around the world (source : Ministry of Science and ICT)

3) Comparative analysis of Korea and overseas cloud market

It is a stage where Korean companies are stating to migrate to the cloud in earnest, and the factors that hinder industrial activation are the first place in introduction cost, the second place security, the third place uncertainty in performance, and the fourth place lack of service model information.

Although the system has been improved to use the private cloud, there is still a limit to the acceptable rage compared to the cloud powerhouse, and the transition to the private cloud is in its infancy due to insufficient financial support and lack of awareness.

The cloud of overseas companies is common and is expanding its influence all over the world.

All major cloud companies opened data centers in Korea and promoted aggressive sales, diversifying the competitive landscape of the cloud market.

In common, the cloud market is being reorganized around SaaS, which has low introduction cost, excellent accessibility, and easy application of new technologies.

The overseas cloud market consists of SaaS(63.6%), laaS(21%), and PaaS(15.4%), while the Korean cloud market consists of SaaS(51.4%), laaS(39.4%), and PaaS(9.1&)

Classification	Overseas Market	Korean Market
Public	• Priority introduction of central government private cloud • Private cloud use without domain restrictions	• Priority introduction of public institutions private cloud • Use of private cloud mainly for public service
Industry	• Changes in cloud market structure with a smooth SaaS-centric transition	• Insufficient SaaS-centric shift • The technical difficulties of SaaS transition and the burden of changing the corporate revenue structure
Ecosystem	• By providing advanced technology convergence services such as data, artificial intelligence, and IoT on the platform, we are breaking down the boundaries between IaaS and PaaS and expanding our own ecosystem	• Expand SaaS and strengthen the cooperative ecosystem between infrastructure-service companies through a cloud flagship project that develops various services in cooperation with a number of cloud companies centering on cloud infrastructure companies

Figure 6. Korea and overseas cloud market comparison table (source : Ministry of Science and ICT)

4) Considerations for Cloud Adoption

Key considerations for the cloud industry include:

1. An alternative method, such as the use of multi-cloud, is needed when a cloud service provider considers its own service termination and disaster recovery.

2. Information technology that supports cloud services has the highest proportion of required competencies when hiring a cloud service provider, suggesting that there is a shortage of ghig-level manpower across the cloud.

A high-level manpower who understands the cloud as a whole and possesses the relevant competency is needed rather than manpower with skills in one filed of software or information system.

3. The division of the scope of responsibility for security between the cloud service provider and the customer should be clear.

Responsibilities vary according to laaS and PaaS, and n the case of laaS, the customer is responsible for most security other than physical security. In the case of SaaS, most of the responsibility for security directly related to the operation of IT infrastructure rests with the cloud service provider.

However, as cloud utilization is developing in the form of hybrid and multi-cloud recently, an intelligent solution is required.

4. Cloud computing is based on an infrastructure that consists of platforms of various companies on a complex network and operates.

In order to solve the system's vulnerability due to complexity and diversity, security technology differentiated from existing on-premises computing is required

Data security is still emerging as the biggest barrier in the cloud industry. In many surveys, when it comes to the top consideration when adopting the cloud, most do not hesitate to mention 'security'.

The same goes for the transition to a public cloud as well as the adoption of a private cloud. Considering the basic properties of the cloud, such as automation of resource management and distributed deployment of workloads with the public cloud, a slightly different approach to security issues is required from the existing on-premises computing .

In conclusion, the big difference between on-premises and cloud is whether the IT resources used to provide services are managed. In the case of on-premises, the service provider directly manages IT resources. In the case of the cloud, the service provider only uses IT resources, and the cloud service provider (CSP) is the subject of resource management.

Major security issues

The government is actively creating an ecosystem to revitalize the cloud, which is the core infrastructure of the digital new deal business that is growing after the post-COVID19. As the cloud serves as the basis for the advancement of data and Al, the core task of the Digital New Deal, it is necessary to pay attention to cloud security issues.

The major security issues in the cloud are as follows.

1. Unauthorized access

In most cases, it is the most threatening security issue in the operation of IT infrastructure . This is a problem that can occur even among internal operators, where the scope of permission is clearly defined by security level, especially when operator permission access from various devices such as personal PCs, smartphones, and tablets is allowed outside the physically restricted scope. This is bound to become weak. When a company uses a public cloud, there are many cases in which the company has a cloud operator inside the company or operates the cloud through an external professional service. This is the reason that various levels of access rights are required apart from administrator access rights at the cloud service provider level, and the access paths are inevitably varied. There fore, cloud security issues due to unauthorized access become more diverse than on-premises computing.

2. Cloud application visibility issues

In the case of an application that handles data in the public cloud , if there is access to data beyond the scope of authority, there is no way to verify this even if data is modified or deleted. Ultimately, it is necessary to determine the security breach issue based on data access patterns and results . This is the part that can hold the most hindrance to the adoption of the cloud by enterprises.

3. Vulnerabilities in Application Interfaces (APIs)

When developing cloud-based services, by utilizing various backend functions provided by the cloud through API calls, development efficiency and scalability during service launch can be increased. It is a trend these days to increase development flexibility by integrating not only functions provided by the cloud, but also functions developed by users through APIs. That's why Microsoft's microservices architecture is getting a lot of attention . Behind this flexibility , it cannot be overlooked that each API call is exposed to security threats. Since any API call can become an attack point for hackers , authorization for API calls and encryption at the time of actual calls are essential.

4. Compliance issues

Different industries and companies have different compliance requirements. In particular, compliance requirements in the public sector are regarded as the biggest obstacle to cloud adoption by governments and public institutions. Organizations that want to introduce the cloud need to analyze these compliance issues first, and prepare in advance such as defining data grades and access rights that comply with regulations.

Response to major security issues

As the cloud market grows, the related security market is also expanding.

Although the cloud service provider (CSP) is in charge of security in the infrastructure sector such as computing, storage, database, and network, the security of data, application, operating system, network and firewall settings is the responsibility of the user company and institution.

Methods for strengthening cloud security include SASE, CASB, CWPP, CSPM, CIEM, KSPM, etc.

It is largely summarized into two categories : Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP).

1. CWPP (Cloud Workload Protection Platform)

With the growing importance of cybersecurity, Cloud Workload Protection Platform (CWPP) is emerging the most to protect cloud environments.

The main purpose of CWPP is to protect server workloads in hybrid and multi-cloud environments, to gain visibility into workloads, and to defend against att acks. According to Gartner, CWPP provides consistent control and visibility into physical computers, virtual machines, containers, serverless workloads, and more. In addition, system integrity protection, microsegmentation of access areas, memory protection, use r behavior monitoring, host-based intrusion prevention, and malware prevention are emerging as a way to proactively respond to workloads from attacks occurring in the area where programs are running.

2. CSPM (Cloud Security Posture Management)

CSPM aims to assess and manage risk facto rs for cloud service configuration.

Automatically identifies and alerts you to misconfiguration or compliance risks. Gartner describes CSPM as a security product that automates security and assures compliance. This reduces the possibility of data leakage and protects the cloud environment.

Summary and implications

So far, we have looked at the current state of the cloud industry. It is possible to understand the overall trend by comparing the Korea and overseas cloud industries, and it can be understood that the world has high interest in the cloud industry through the market share that increases every year.

In the future, enterprises adopting or spreading the cloud will find it difficult to avoid going to hybrid and multi- cloud. In order to take full advantage of the artificial intelligence and big data technologies and various backend functions provided by existing cloud service providers while simultaneously accommodating the compliance requirements of public institutions and major security issues, it may be necessary to mix dedicated private clouds and multiple public cloud providers.

Cloud market growth and security threats are proportional. For cloud security, security must be applied at the same time as the cloud is introduced.

In the case of the Korea cloud market, it can be seen that the cloud market is maturing as cloud adoption is recognized as a business investment rather than cost reduction.

In the future, it is expected that Korean companies will accelerate the data and artificial intelligence economy through full-scale cloud conversion and leap into a full-fledged digital leading country .

By clearly understanding the current status of the cloud, which has become a key keyword in the IT industry, preparing for changes in all environments surrounding IT, such as organization, culture, technology, and governance, and securing competitiveness for the sustainable growth of the next generation cloud industry is important.

KR CS++

No.	Titles
1	Understanding of Maritime Cyber Security
2	Practice of Maritime Cyber Security
3	Administrative Security
4	Cyber Asset, Threat and Technical Security
5	KR Cyber Security Type Approval
6	Understanding of Maritime Cyber Security Risk Assessment
7	KR Remote Cyber Survey

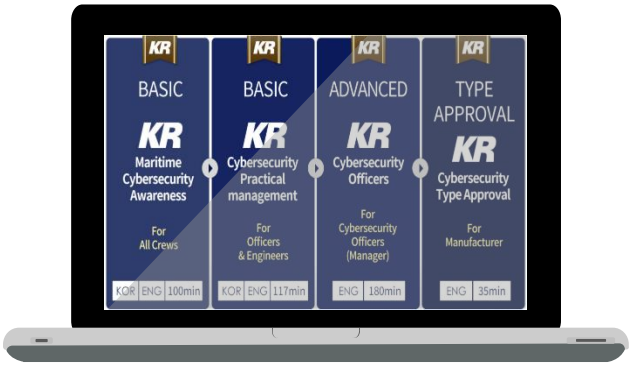
KR launched KR CS++, maritime cybersecurity training tool.

KR CS++ was produced in USB type and tablet type for effective cybersecurity training of seafarers in an environment where cybersecurity training is difficult due to the unstable Internet environment on ships. In addition, KR is striving for customer satisfaction by providing various types of services.

Currently, the same service is provided through cybersecurity e-learning education.

Online Training

KR Maritime Cybersecurity e-Learning Center training course



Q&A : https://edu.orangecq.com/

KR reorganized the cyber security e-learning training in cooperation with Orange Security, who is a maritime cyber security specialist. Through this reorganization of e-learning training, KR becomes to provide customized training for each customer.

New curriculum consists of Maritime cyber security Awareness, cyber security Practical Management, cyber security Officers and cyber security Type Approval. Maritime cyber security Awareness is a course to raise awareness of maritime cyber security for employees including crews, which includes two modules - Understanding of Maritime Cyber Security and Practice of Maritime Cyber Security. cyber security Practical Management is a course for ship officers and engineers, which includes KR Remote Cyber Survey as well as Maritime cyber security Awareness course. cyber security Officers is for the person in charge of managing cyber security system and responding classification cyber security survey. This course consists of Administrative Security, Cyber Asset, Threat and Technical Security, Understanding of Maritime Cyber Security Risk Assessment with all modules in cyber security Practical Management. Finally, KR Cyber Security Type Approval is a course for equipment company and provides introduction of international standard related to requirements of cyber security for equipment and materials required for obtaining KR cyber security type approval.

Providing the best services, Creating a better world

Cyber Certification Team, Korean Register
(46762) 36, Myeongji ocean city 9-ro, Gangseo-gu, Busan Republic ok Korea
Tel +82 70 8799 8595
Fax +82 70 8799 8594
www.krs.co.kr