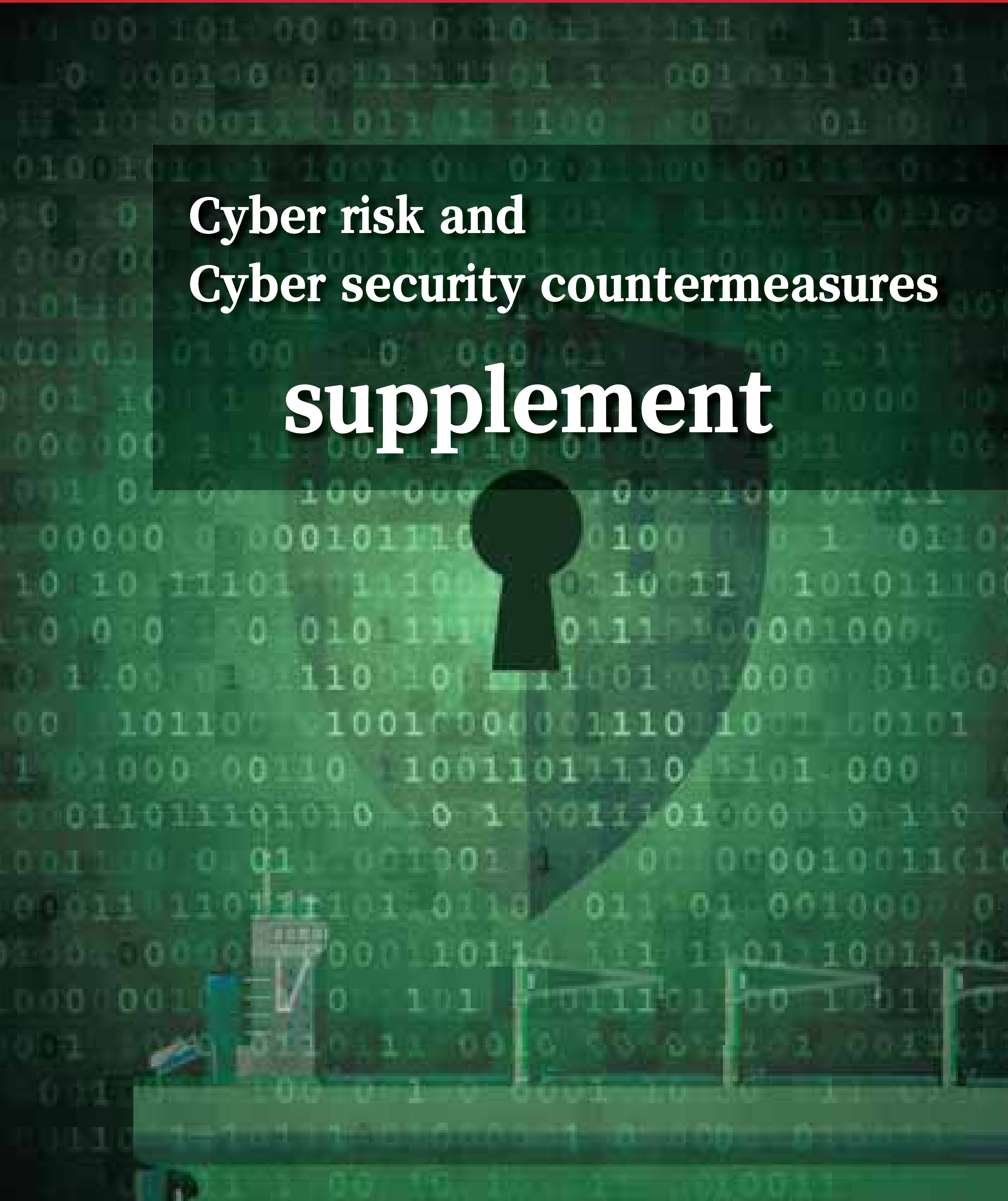
JAPAN P&I CLUB Vol.48 May 2020

P&I Loss Prevention Bulletin

The Japan Ship Owners'Mutual Protection & Indemnity Association Loss Prevention and Ship Inspection Department

Cyber risk and Cyber security countermeasures

supplement



Index

Appendix

Introduction

In early 2020, we heard the news of cyberattacks against the four leading companies of Japan's defense and infrastructure industries. In the maritime industry as well, the threat of cyberattacks has increased rapidly because of the problems of GPS spoofing that occurred in certain specified areas, etc.

According to IMO guidelines, ship owners and ship managers are required to address cyber risks appropriately in the Safety Management System (SMS) no later than the first annual verification of the Company's Document of Compliance after 1 January 2021. Although the requirements are not mandatory, flag state administrators request their respective vessels to follow the guidelines accordingly.

With regard to the latest cyber attacks, we would like to introduce some case studies on ship operations in this bulletin as a supplement to our Loss Prevention Bulletin Vol.42 "Cyber risk and Cyber security countermeasures". We hope this will assist you in establishing and reviewing cyber security countermeasures.

IMO circulars

Maritime Safety Committee (MSC), 94th session, November 2014

The Committee considered a proposal to develop voluntary guidelines on cyber security practices to protect and enhance the resiliency of cyber systems supporting the operations of ports, vessels, marine facilities and other elements of the maritime transportation system and agreed to coordinate its future work on this matter with the Facilitation Committee.

Maritime Safety Committee (MSC), 96th session, May 2016

The Maritime Safety Committee, at its ninety-sixth session, having considered the urgent need to raise awareness on cyber risk threats and vulnerabilities, approved the interim guideline MSC.1/Circ.1526 on maritime cyber risk management.

The interim guidelines are intended to provide high-level recommendations for maritime cyber risk management, although there was no specified standard for each system, device and piece of equipment. The Guidelines also include factors to take into account when considering cyber risk management.

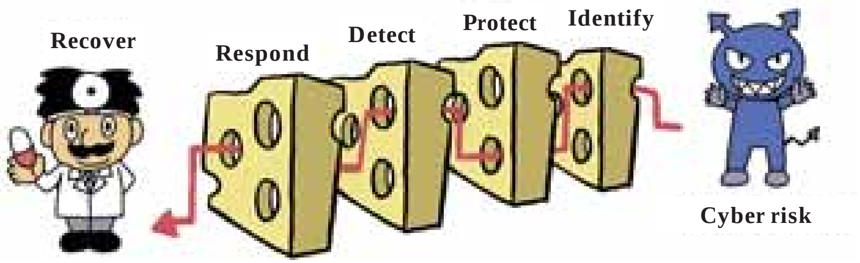
Maritime Safety Committee (MSC), 98th session, June 2017

The Maritime Safety Committee, at its ninety-eighth session in June 2017, adopted Resolution MSC.428(98)) - Maritime Cyber Risk Management in Safety Management Systems, recommended that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM

Code. With regard to guidelines on maritime cyber risk management, the Facilitation Committee and the Maritime Safety Committee updated the interim guidelines contained in MSC.1/Circ.1526, the contents of which were approved in MSC-FAL.1/Circ.3

The IMO guidelines set out the following elements in support of an effective cyber risk management strategy:

- **Identify**: Define the roles responsible for cyber risk management and identify the systems, assets, data and capabilities that, if disrupted, pose risks to ship operations.
- **Protect**: Implement risk control processes and measures, together with contingency planning to protect against a cyber incident and to ensure continuity of shipping operations.
- **Detect**: Develop and implement processes and defenses necessary to detect a cyber incident in a timely manner.
- **Respond**: Develop and implement activities and plans to provide resilience and to restore the systems necessary for shipping operations or services which have been halted due to a cyber incident.
- **Recover**: Identify how to back-up and restore the cyber systems necessary for shipping operations which have been affected by a cyber incident.



Flag State circulars
Class Societies

Flag State circulars

Panama	Maritime Cyber Risk Management -MERCHANT MARINE CIRCULAR MMC-354
Marshall Islands	Maritime Cyber Risk Management -Maritime Cyber Risk Management No. 2-11-16
LIBERIA	Maritime Cyber Risk Management -MARINE SECURITY ADVISORY – 02/2019

The above flag state administrators request that cyber risks are appropriately addressed in the Safety Management System (SMS) as well as the ISPS in accordance with the IMO guideline.

*Note: please check the latest information of each flag state and class society.

Class Societies

In 2019, as part of the ClassNK Cyber Security Series, ClassNK released the following guidelines and standards:

“*Guidelines for Designing Cyber Security Onboard Ships*” – for shipyards and shipowners
“*Cyber Security Management System for Ships*” – for ship management companies and ships
“*Software Security Guidelines*” – for shipboard equipment manufacturers

Besides, ClassNK consulting service Ltd., a subsidiary company of ClassNK, started an online course on cyber security education in March 2020. The program is available in both English and Japanese and is certified by ClassNK in compliance with the Guidelines on Cyber Security Onboard Ships Version 3

BIMCO Cyber Security Clause 2019

The BIMCO Cyber Security Clause 2019 is designed to mitigate cyber security incidents, and stipulates an obligation to implement appropriate cyber security systems, and to detect cyber risks to protect related parities. (The full text of the clause is in the back of this Bulletin)

Subclause (a) sets out that the parties are required to implement “appropriate” cyber security measures and systems.

Subclause (b) requires the parties to use reasonable endeavours to ensure any third party performing services on their behalf has in place proper cyber security (i.e. shipbrokers and agents provide services and information to owners and charterers digitally).

Subclause (c) requires the notification is to be given by the party who comes aware of a cyber security incident. If one party is affected by a cyber security incident, it is obliged to inform the other party and provide alternative contact details and any information available that might help to mitigate or prevent the effects of the incident within 12-hours.

Subclause (d) contains a limitation of liability and provides a blank space to be filled out with the liability cap. A default limit of USD 100,000 will apply if the parties do not to fill in an amount. If an incident giving rise to a claim is the sole result of gross negligence or wilful misconduct of a party, the liability cap is excluded.

Summary from 39th session “*Work shop Maritime Charter Party*” by Yoshida & Partners

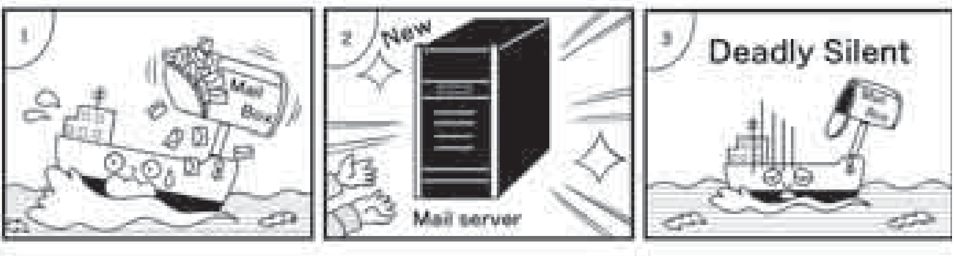
Cyber attacks are becoming more sophisticated day by day, and it is of utmost importance that a vessel in danger of being exposed to a cyber incident reports this to both relevant parties and the IT managers as urgently as possible to obtain instructions in order to mitigate any damage. Thus, the first step is to report the incident.

Case studies

Case 1

Charter's e-mails were being blocked by the Anti-Spam Server which had been newly installed by the owner.

Causation Misdetection of spam e-mails, the absence of a network manager



Case 2

Newly installed e-mail scanning Anti-Virus software affected smooth communication on board

Causation Without any verification test, the company provided the same type of Anti-Virus as ashore

Case 3

The password of the ship's PC was leaked, because the Master became a victim of a phishing attack.

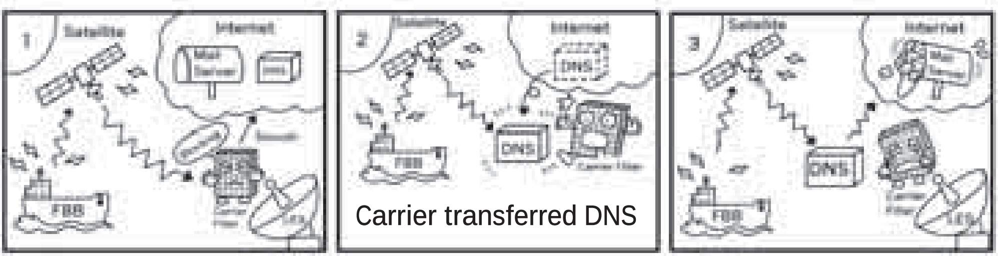
Causation The IE and OS installed on the ship's PC was not up-to-date. The Master had a lack of IT literacy.

1
2
Password
3
ID
Password

Case 4

Satellite communication cost greatly increased : Monthly traffic suddenly increased by 100 Mb.

Causation Satellite communication carrier changed the position of the DNS server without any notice.



Case 5

Ship’s LAN stopped working.

Causation A subcontractor misconnected computers/cables to the communications LAN when installing a ship monitoring camera system.

Case 6

Ship’s LAN stopped working

Causation Seafarers set up a private wireless network access point without permission, which affected the business use LAN.

1
One day
Ship's network speed is very slow... booster can be...
Crew
2
This made it better...
Crew
3
Network error
Offical PC
Captain's room

Case 7

Ship’s LAN connection became unstable

Causation After delivery from the dockyard, the ship’s LAN connection had become physically unstable due to ship vibration. This is because the connection between LAN cable and LAN port had been poorly crimped at the dockyard.

Case 8

Satellite communication was lost after upgrading the ECDIS application software

Causation The IT manager did not know that the port number had been changed at the time of software upgrade, because the SI in charge did not notify the IT manager of the change.

Case 9

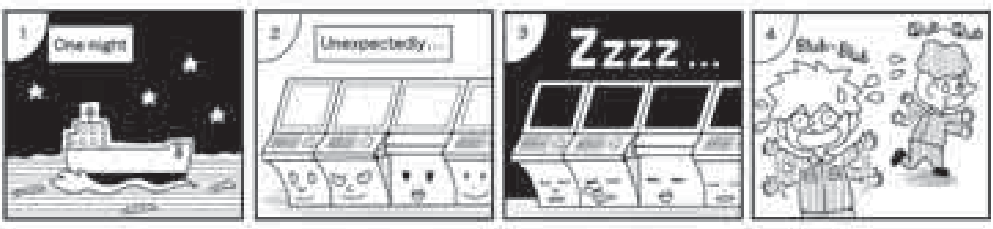
After the installation of VSAT, the sending and receiving of e-mails became unstable due to data speed limits

Causation Although the owner decided to use the VSAT carrier unlimited data plan, this did not include Committed Information Rate (CIR), and there were problems with exchanging necessary emails between the ship and shore offices under such a limited speed rate.

Case 10

Suddenly four ECDIS systems and three RADARs shut down during night navigation underway to Chinese ports.

Causation Some days later, it was discovered by a shore technician that there were configuration problems regarding equipment system integration (including primary/secondary system settings between ECDIS units).



Observations by ship inspections and external audits on board

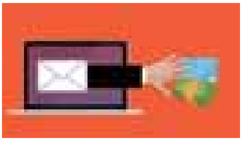
Regarding the below-mentioned observations, it is recommended that any effective action should be taken in accordance with risk assessment advice or feedback from IT managers.

1 ***There is no Cyber Security Response Plan in the procedure manual.***

2 ***There were no port covers for USB and LAN ports on computers and/or other devices.***

3 ***Updates on the OS of ship's computers had not been performed. Instead, an older version of OS for which maintenance support had ended was being used.***

4 ***A test on phishing had not been carried out.***



5 ***A test on third party penetration had not been carried out.***

Considerations

1
May I print out port entry docs on board?
sure
thanks
Agent
Ship'sPC
Crew
2
Ship port entry……
3
Few days later
No Data

During actual ship operations, the following are examples of how every network and computer on board can be infected with a computer virus:

- Some crew may be asked to print a maintenance or repair service report by an external engineer.
- Some crew may intend to use the data file of a ship or to save data on a computer shared with the other crew on board, using a non-company owned and/or a non-recognized USB flash drive.
- Some crew may connect a personal smar tphone to an on-board wireless network.

How do you design and implement successful cyber security management? Provide your vessel with some device that enables the safe and two-way transfer of data between networks, and any appropriate procedure for coping with the above-mentioned cases, as well as to implement education and training for crew.

In addition, it could be that the SI in charge was not up-to-date regarding IT, the latest software or how to operate the ECDIS system. This is something that the onboard ship inspection or audit should have identified.

Looking over the case studies provided in this bulletin, it is clear to see that the majority of cyber incidents are caused by the lack of proper measures and adequate education that should be based on cyber security management and applicable to both companies and their crews.

On the other hand, we need to consider the impact of the social media on crews' life at sea. The usage of social networking services has actually caused many problems, namely: the leakage of information on confidential shipping matters, diffusion of marine accident information and photos without a company's permission, posting of the contents of unsafe actions on board, the exposure of personal private information, and so on. Therefore additional attention should be paid to security management implemented at an individual crew level.

Further, it has been noted that crew were making money trading private Wi-Fi capacity onboard, which may compromise crew harmony.

Regarding tips on managing cyber security risks, we recommended that an IT manager be assigned in our Bulletin Vol.42 published in May 2018. In reality, it was revealed that there was no implementation of an IT policy, assignment of an IT manager, or rule for social media that crew must follow in nearly 60% of shipping companies according to the survey that we conducted in our spring domestic seminar 2019.

As described previously, the roles and responsibilities of an IT manager are important, especially when response to any emergency is required, and the installation or maintenance of computers and software should be performed by IT managers that regularly visit operating vessels. If a suitable person for cyber security management cannot be found in your company, it is suggested that, as an effective measure, you establish a system whereby you can consult directly with external experts.

We hope that this Loss Prevention Bulletin will be put to good use in your establishment of cyber security countermeasures.

<Remarks>

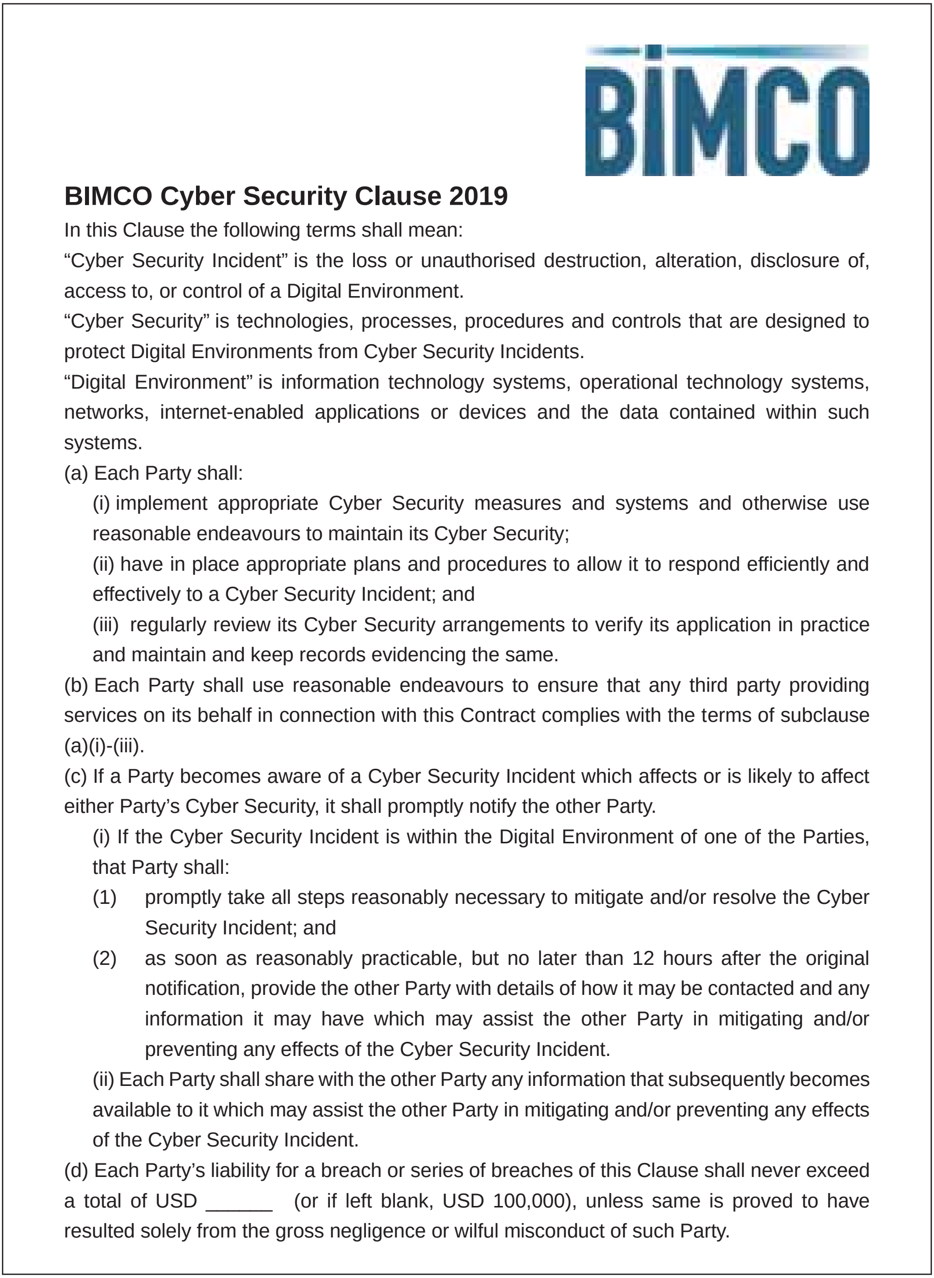
The contents in this bulletin were compiled with the co-operation of ORCA CO., LTD. (Http://www.orcajpn.co.jp/index.html).

Reference

- IMO
- The Guidelines On Cyber Security Onboard Ships ver3
- Maritime Cyber Risk Management -MERCHANT MARINE CIRCULAR MMC-354
- Maritime Cyber Risk Management -Maritime Cyber Risk Management No. 2-11-16
- Maritime Cyber Risk Management -MARINE SECURITY ADVISORY – 02/2019

Appendix

- BIMCO Cyber Security Clause 2019
- Draft Area no. 28 Cyber security in Dry Bulk Management Standard
- Cyber Security Management Poster



BIMCO Cyber Security Clause 2019

In this Clause the following terms shall mean:

“Cyber Security Incident” is the loss or unauthorised destruction, alteration, disclosure of, access to, or control of a Digital Environment.

“Cyber Security” is technologies, processes, procedures and controls that are designed to protect Digital Environments from Cyber Security Incidents.

“Digital Environment” is information technology systems, operational technology systems, networks, internet-enabled applications or devices and the data contained within such systems.

(a) Each Party shall:

(i) implement appropriate Cyber Security measures and systems and otherwise use reasonable endeavours to maintain its Cyber Security;

(ii) have in place appropriate plans and procedures to allow it to respond efficiently and effectively to a Cyber Security Incident; and

(iii) regularly review its Cyber Security arrangements to verify its application in practice and maintain and keep records evidencing the same.

(b) Each Party shall use reasonable endeavours to ensure that any third party providing services on its behalf in connection with this Contract complies with the terms of subclause (a)(i)-(iii).

(c) If a Party becomes aware of a Cyber Security Incident which affects or is likely to affect either Party’s Cyber Security, it shall promptly notify the other Party.

(i) If the Cyber Security Incident is within the Digital Environment of one of the Parties, that Party shall:

(1) promptly take all steps reasonably necessary to mitigate and/or resolve the Cyber Security Incident; and

(2) as soon as reasonably practicable, but no later than 12 hours after the original notification, provide the other Party with details of how it may be contacted and any information it may have which may assist the other Party in mitigating and/or preventing any effects of the Cyber Security Incident.

(ii) Each Party shall share with the other Party any information that subsequently becomes available to it which may assist the other Party in mitigating and/or preventing any effects of the Cyber Security Incident.

(d) Each Party’s liability for a breach or series of breaches of this Clause shall never exceed a total of USD ______ (or if left blank, USD 100,000), unless same is proved to have resulted solely from the gross negligence or wilful misconduct of such Party.

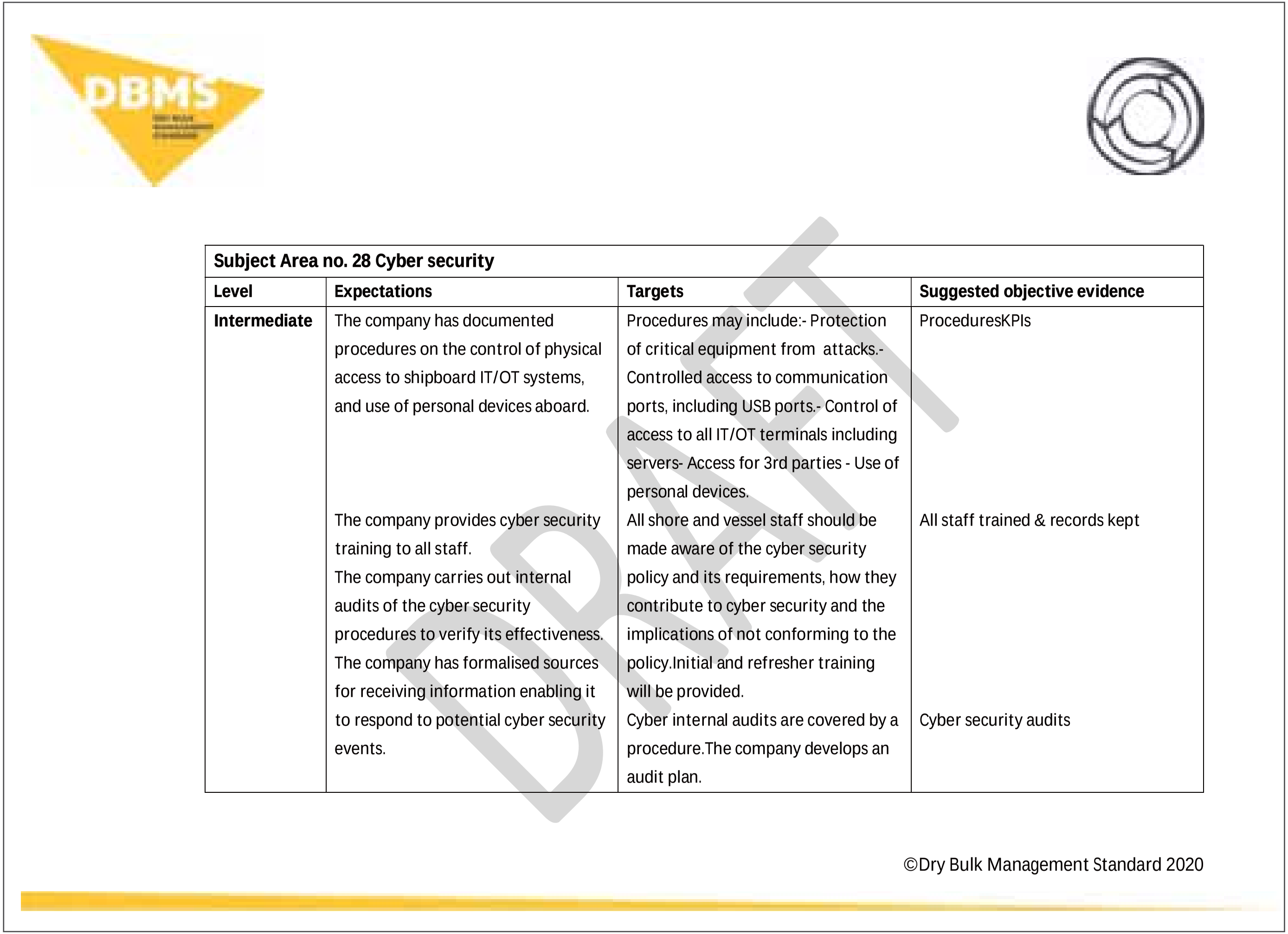
Draft Area no. 28 Cyber security in Dry Bulk Management Standard

In April 2020, the new Dry Bulk Management Standard (DBMS) to support the improvement of safety was launched. (The standard is still in draft format). The standard provides dry bulk segmentation benchmarks (four levels: basic, intermediate, advanced and excellent).

This will assist you in establishing and reviewing cyber security countermeasures.

Subject Area no. 28 Cyber security			
Principle: The company has a programme to design and operate IT and digital process control systems to manage risk to system and information integrity, availability and confidentiality.			
Level	**Expectations**	**Targets**	**Suggested objective evidence**
Basic	The company has documented policy and procedures covering cyber security.	The policy, which is signed by senior management, includes a commitment to minimising the impact of cyber incidents.	Policy and procedures
	The company has carried out cyber security assessments, and has developed a cyber security plan.	The assessment could include: identification of external and internal cyber security threats, identification of onboard IT and OT with communications links, identification of the consequences of a cyber security threat on these systems.	Cyber security assessments Cyber security plan Procedures to recover from incident
	The company has procedures in place for responding to and recovering from cyber incidents.		
	The company has designated appropriate shore based and ship based personnel with responsibility for cyber security.	The plan includes measures to: reduce the likelihood of vulnerabilities being exploited, reduce the potential impact of a vulnerability being exploited.	Responsibility designated ashore and aboard Training and qualifications.

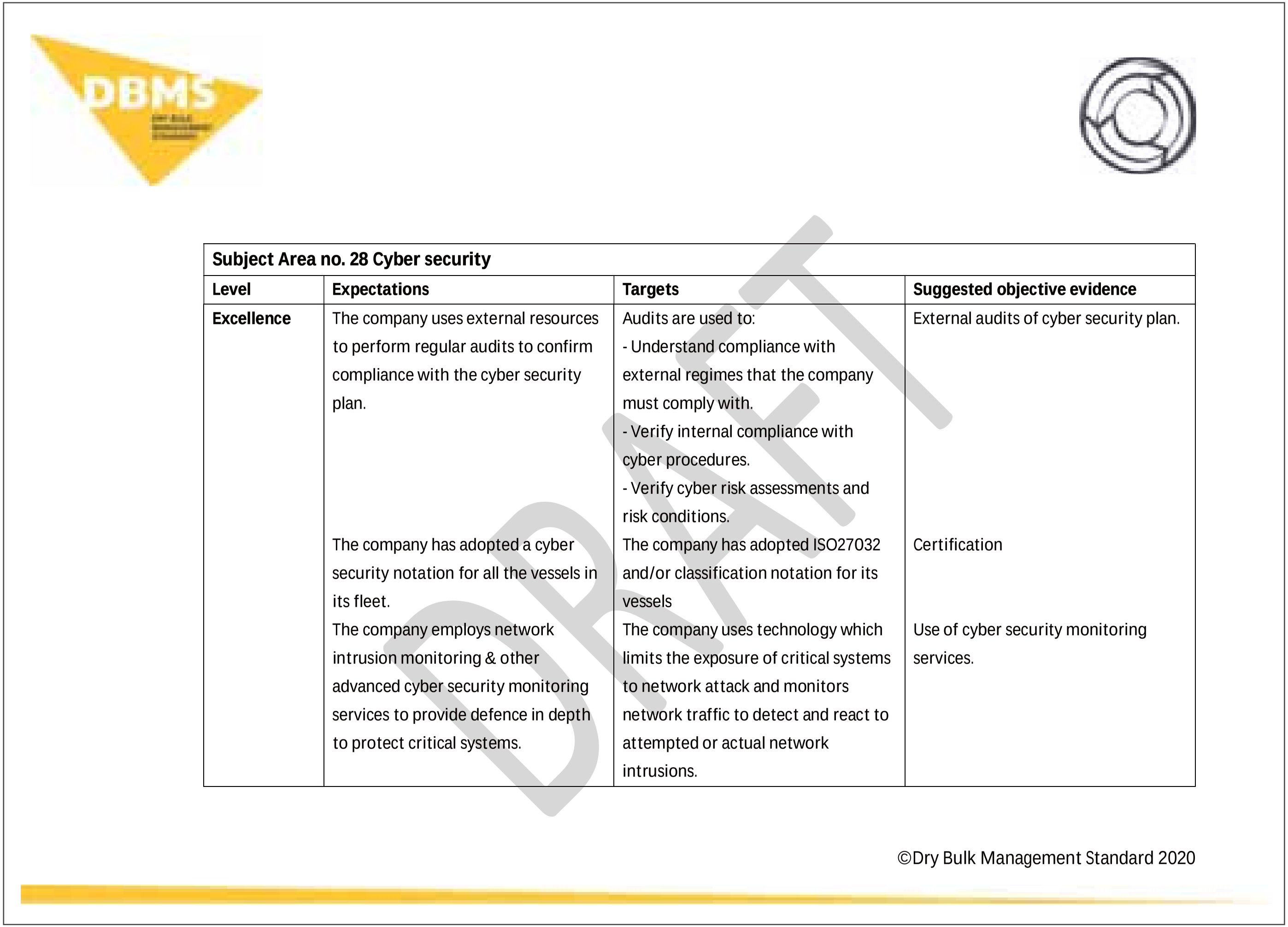
©Dry Bulk Management Standard 2020



Subject Area no. 28 Cyber security			
Level	**Expectations**	**Targets**	**Suggested objective evidence**
Intermediate	The company has documented procedures on the control of physical access to shipboard IT/OT systems, and use of personal devices aboard. The company provides cyber security training to all staff. The company carries out internal audits of the cyber security procedures to verify its effectiveness. The company has formalised sources for receiving information enabling it to respond to potential cyber security events.	Procedures may include:- Protection of critical equipment from attacks.- Controlled access to communication ports, including USB ports.- Control of access to all IT/OT terminals including servers- Access for 3rd parties - Use of personal devices. All shore and vessel staff should be made aware of the cyber security policy and its requirements, how they contribute to cyber security and the implications of not conforming to the policy.Initial and refresher training will be provided. Cyber internal audits are covered by a procedure.The company develops an audit plan.	ProceduresKPIs All staff trained & records kept Cyber security audits

Subject Area no. 28 Cyber security

Level	Expectations	Targets	Suggested objective evidence
Advanced	The company reviews effectiveness of its cyber security plan to ensure its suitability, adequacy and effectiveness.	Management reviews should be carried out at least annually in order to follow-up the implementation and development of the plan.	Documented management reviews
	The company enforces third party access management.	The company takes appropriate precautions for third party access to IT and OT. The company performs due diligence audits or uses independent auditors reports before granting access to systems.	3rd party access precautions. Due diligence audits.
		Vessel and equipment are designed and engineered to minimise cyber vulnerabilities. The company has a formal process before employing new technology aboard its fleet	Cyber security assessments for new equipment.

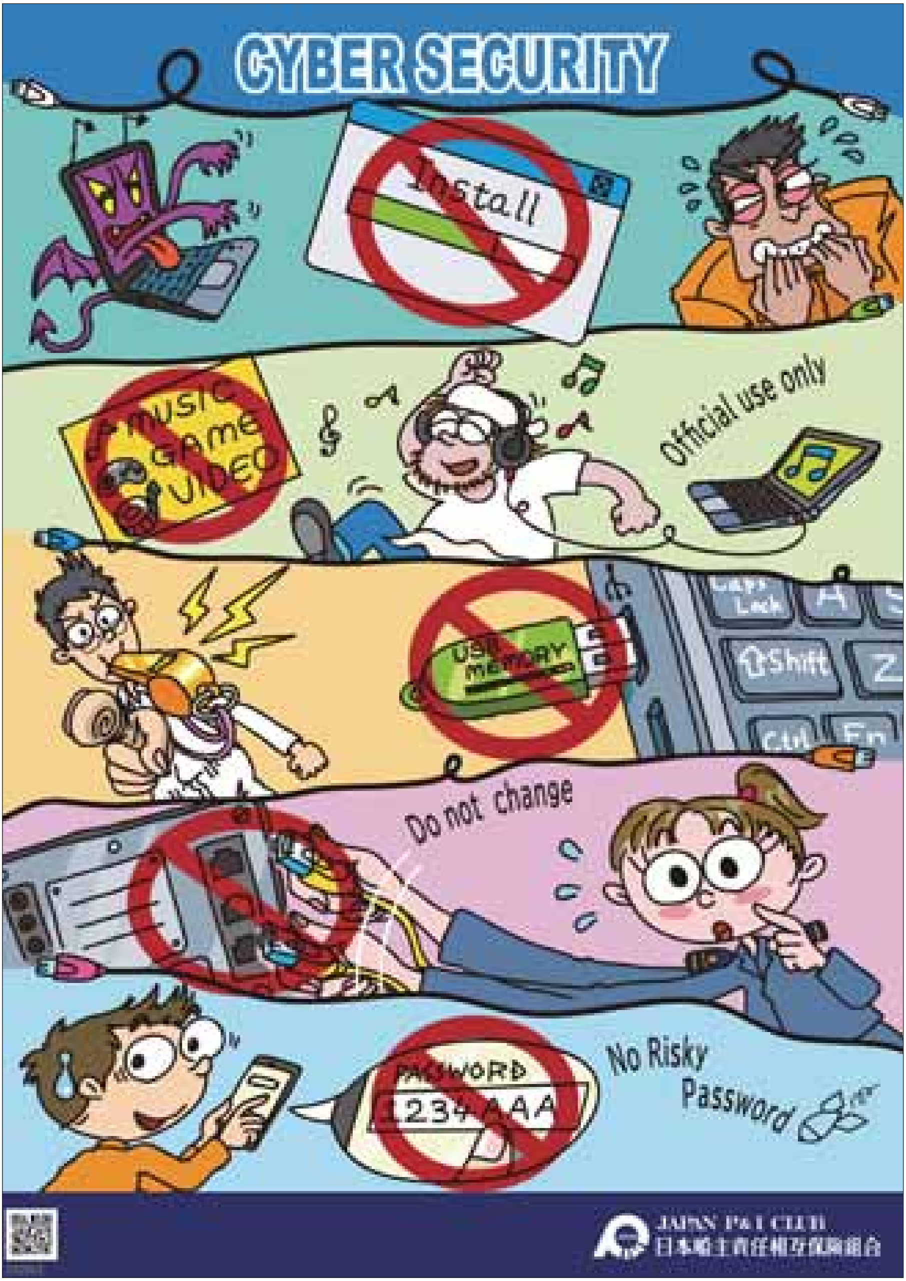


Subject Area no. 28 Cyber security			
Level	**Expectations**	**Targets**	**Suggested objective evidence**
Excellence	The company uses external resources to perform regular audits to confirm compliance with the cyber security plan.	Audits are used to: - Understand compliance with external regimes that the company must comply with. - Verify internal compliance with cyber procedures. - Verify cyber risk assessments and risk conditions.	External audits of cyber security plan.
	The company has adopted a cyber security notation for all the vessels in its fleet.	The company has adopted ISO27032 and/or classification notation for its vessels	Certification
	The company employs network intrusion monitoring & other advanced cyber security monitoring services to provide defence in depth to protect critical systems.	The company uses technology which limits the exposure of critical systems to network attack and monitors network traffic to detect and react to attempted or actual network intrusions.	Use of cyber security monitoring services.

Notes:

Cyber Security Management Poster

Periodical check radar overlay
JAPAN P&I CLUB
日本船主責任相互保険組合


CYBER SECURITY
Install
music
GAME
VIDEO
Official use only
USB MEMORY
Caps Lock
A
S
⇧Shift
Z
Ctrl
Fn
Do not change
PASSWORD
1234AAA
No Risky Password
JAPAN P&I CLUB
日本船主責任相互保険組合

The author

Takehiko Hino / Manager
Loss Prevention and Ship Inspection Dept.
The Japan Ship Owners' Mutual Protection & Indemnity Association

JAPAN P&I CLUB
日本船主責任相互保険組合

Website www.piclub.or.jp

● **Principal Office（Tokyo）**
2-15-14, Nihonbashi-Ningyocho Chuo-ku, Tokyo 103-0013, Japan
Tel：03-3662-7229 Fax：03-3662-7107

● **Kobe Branch**
6th Floor Shosen-Mitsui Bldg. 5, Kaigandori Chuo-ku, Kobe, Hyogo 650-0024, Japan
Tel：078-321-6886 Fax：078-332-6519

● **Fukuoka Branch**
6th Floor Meiji-Dori Business Center 1-1, Shimokawabata-machi, Hakata-ku, Fukuoka 812-0027, Japan
Tel：092-272-1215 Fax：092-281-3317

● **Imabari Branch**
2-2-1, Kitahorai-cho, Imabari, Ehime 794-0028, Japan
Tel：0898-33-1117 Fax：0898-33-1251

● **Singapore Branch**
80 Robinson Road #14-01B SINGAPORE 068898
Tel：65-6224-6451 Fax：65-6224-1476

● **Japan P&I Club (UK) Services Ltd**
5th Floor, 38 Lombard Street, London EC3V 9BS U.K.
Tel：44-20-7929-3633 Fax：44-20-7929-7557