JAPAN P&I CLUB Vol.42 May 2018

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

Contents

Text and forms provided by ORCA CO., LTD.

＜ Note ＞

Regarding the text and forms provided by ORCA CO., LTD. which were introduced in this bulletin, ORCA CO., LTD. possess the primary copyright. However, we have permission to duplicate, edit, revise and distribute only for the purpose of Club member SMS manual revision.

＜ Disclaimer ＞

This Loss Prevention Bulletin is issued for the purpose of supporting Club members and related parties with cyber security countermeasure planning. The Japan Ship Owners' Mutual Protection & Indemnity Association and ORCA CO., LTD. are not liable for any damage caused as a result of using this bulletin.

§1 Introduction

The threat of cyber attacks at sea have increased recently and our Club issues a circular entitled “Cyber risk and cyber security” accordingly. The necessity of cyber security countermeasures and guidelines have been set forth by the IMO (MSC-FAL.1/Circ.3 Guidelines on Maritime Cyber Risk Management) and each shipping organization.

1－1 Cyber risk and P&I insurance

Cyber risks have not been specified in the Japan P&I Club rules, however, a claim regarding the coverage of a cyber attack or cyber breach would be examined in the usual way with reference to the Rules. When the cyber attack would not fall under the definition of "war" or "act of terrorism" under rule 35, a member will be subject to cover along with his normal P&I insurance.

Sponsored by FURUNO
New Generated Bridge System Voyager

For example, the following case would normally be subject to P&I insurance: The ship’s system gets infected with a virus via the onboard LAN system via the e-mail PC used for work or a crew member’s personal PC. The onboard PC’s software for work use is updated without permission or, as a result that particular crew member changed connection to the onboard LAN cable without permission. The electronic aid for navigation and propulsion breaks down, which causes damage to harbour facilities at the time of departure.

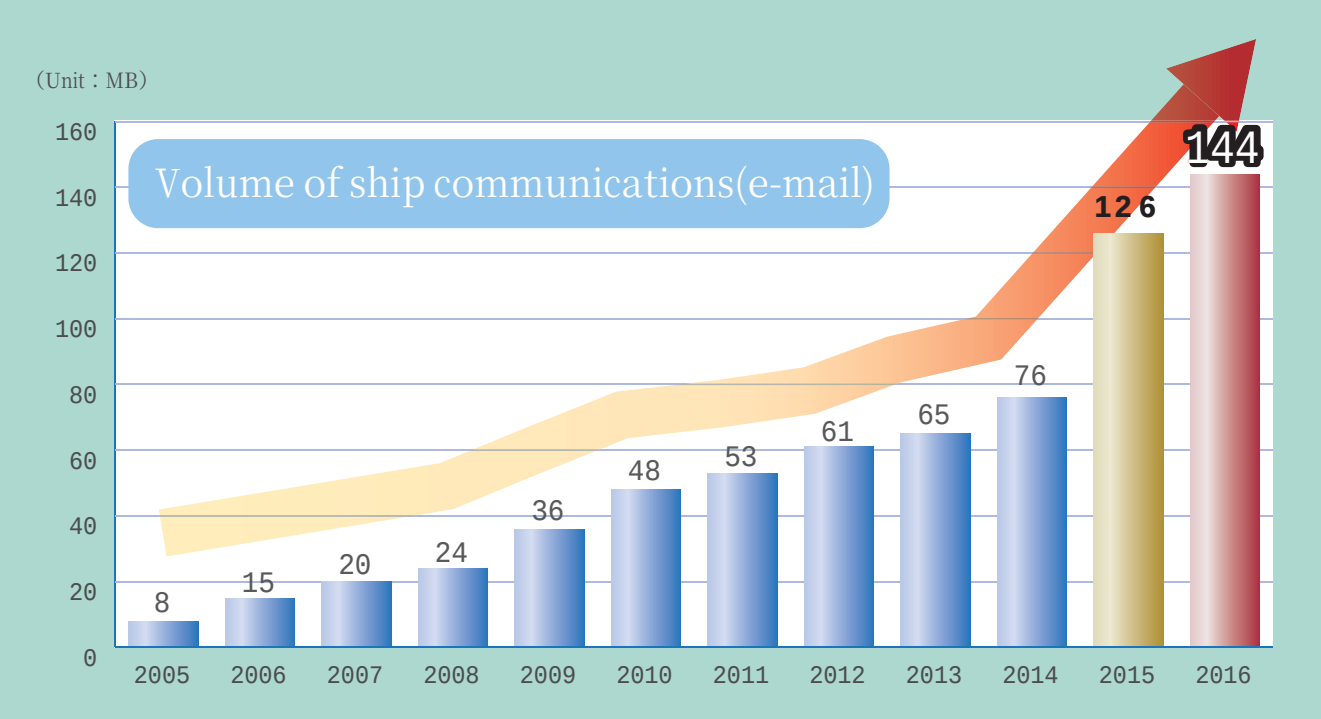
The following examples will not be covered by P&I insurance: For instance, there was a case whereby a certain amount of the ship’s store was transmitted mistakenly due to a hacked e-mail. In another case, the ship’s schedule was delayed because the crew was investigated by the authorities, because the uploaded video which was found in his personal PC appeared to be associated with terrorism. Further, a threatening email was sent to the ship as a fake money demand meaning that the ship might have been arrested. Such cases which do not develop into P&I accidents were reported.

§2 Example of a ship communications system that has been infected with a virus

2-1 Ship communications

Except for GMDSS (Global Maritime Distress and Safety System, which is equipment that is installed on a ship depending on the sea area that is to be sailed), V-SAT, Fleet Xpress, FBB, Iridium, internet using 4G, e-mail, telephones and Faxes are frequently used on the ship. This ship communication equipment is not only a communication tool between ship and shore, but also essential equipment for current navigation, such as weather routing, chart correction and PMS (Planned Maintenance System).

The volume of ship communications via e-mail have increased due to this. Graph 1 shows the volume of ship communications via e-mail by month over the last 12 years. Compared with 2005, the volume of communications in 2016 has increased by 18 times.



Graph 1 Volume of ship communications via e-mail by month over the last 12 years

2-2 Example of a system infected with a virus

On the other hand, along with the volume increase in ship communications, the number of ship systems that are prone to being infected with a virus are also occurring more frequently, and the way in which viruses infect systems are now more varied.

By around the year 2000, ship viral infection was blocked by the e-mail provider. When it came to ship's local network, because most vessels were not initially connected to an external network, there were many cases whereby people or crew who boarded the ship brought viruses on board with them physically.

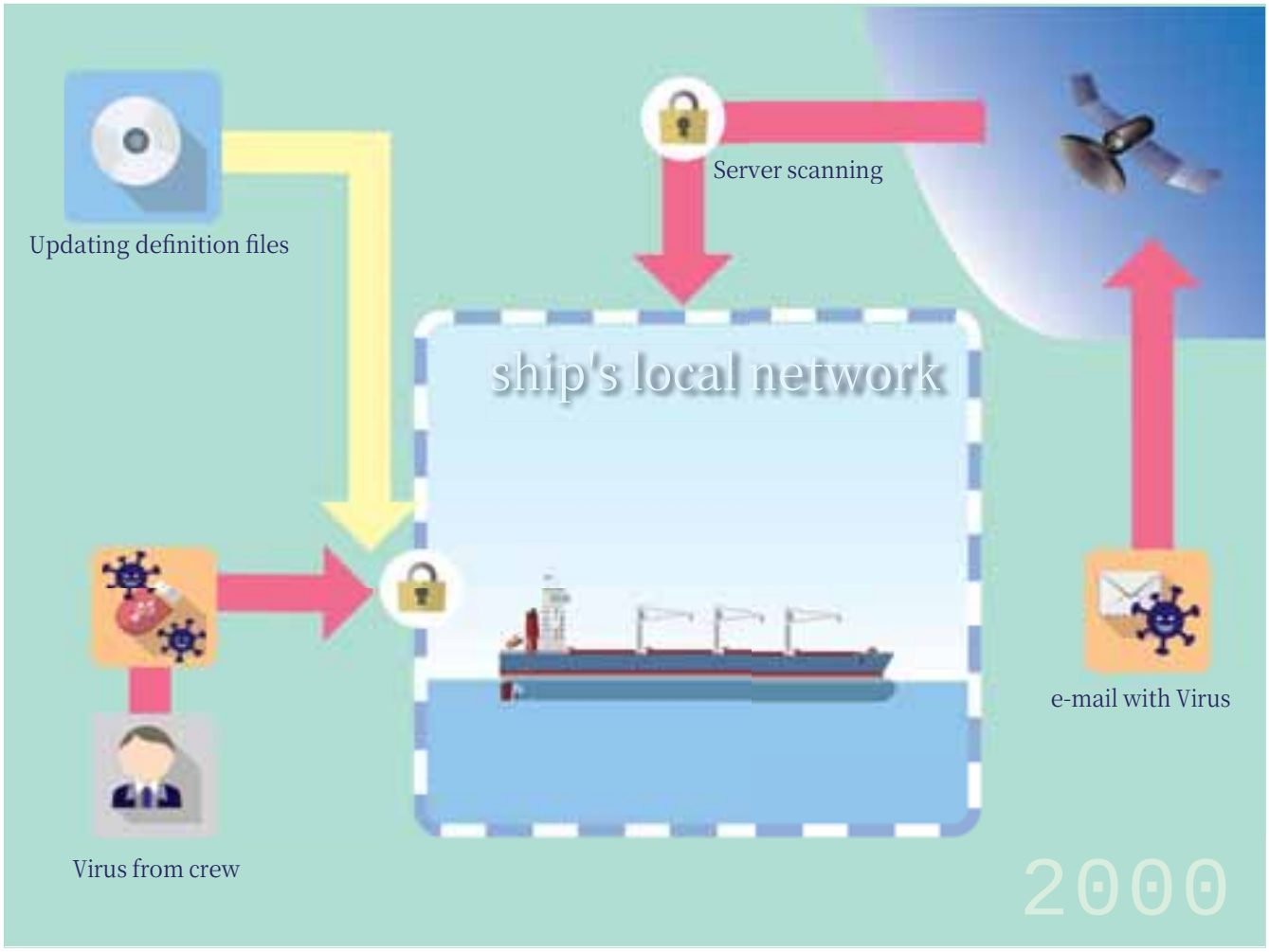


Fig. 2 Around 2000

However, since around 2010, there have been some cases whereby an intrusion of the latest virus caused the ship to be infected and, as a result, disrupted the e-mail system. This came about as a result of a member of crew using 3G/4G when calling at port.

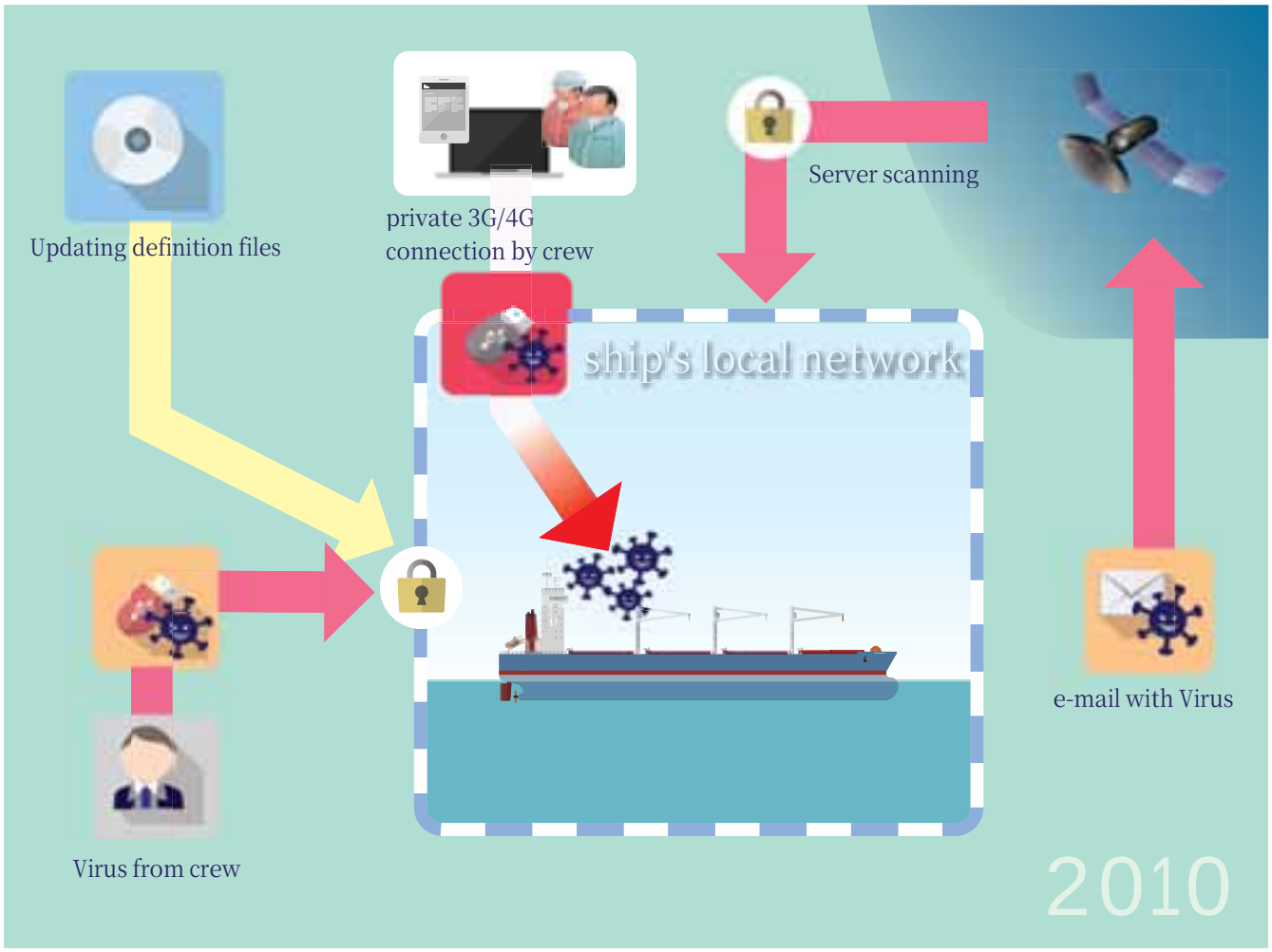


Fig. 3　Around 2010

Actions such as the use of illegally copied software and illegally downloaded sites, as a result, are some of the causing circumstances whereby a system may be easily infected by the latest virus.

It is needless to say that these ship communications devices and their connected onboard PCs, navigation electronics and propulsion equipment etc. are essential when it comes to examining cyber security countermeasures. However, there seems to be little known when it comes to taking a specific approach concerning the examination of risk assessment, revisions to the SMS (Safety Management System) or SSP (Ship Security Plan).

In the last part of this bulletin, we will take a look at ORCA CO., LTD., which has practical accomplishments in the shipping IT field, and introduce a SMS template that simulates the MSC-FAL.1/Circ.3 Guidelines on Maritime Cyber Risk Management, using the risk assessment approach method for cyber security countermeasures.

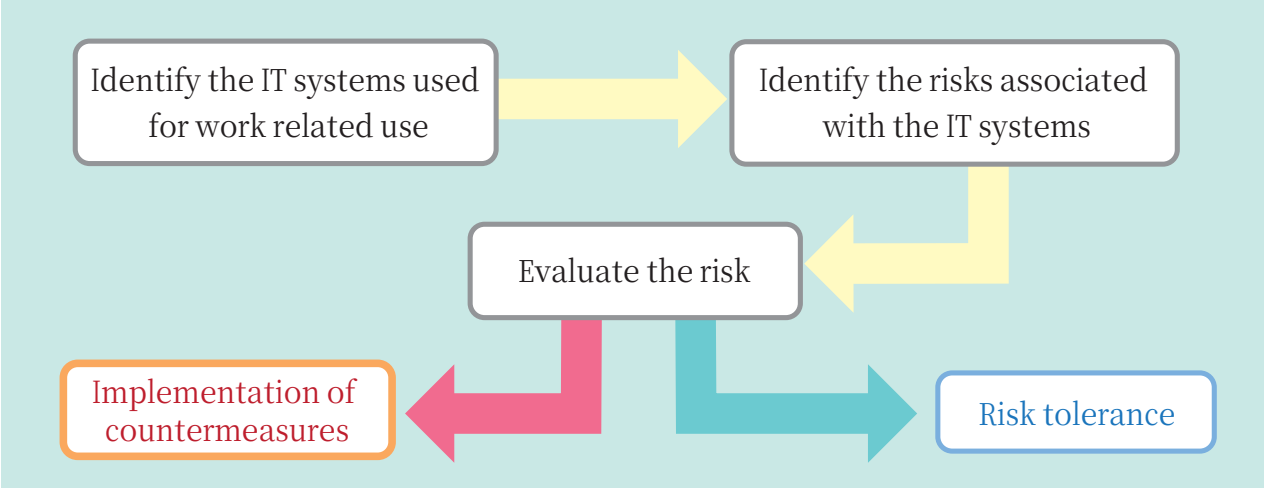
§3 Preparation needed to manage cyber security countermeasures

3－1 How to prevent cyber risk

Here, we would like to define cyber risk as potential factors which may cause problems or affect the IT system which may even also cause disorder in the carrying out of duties and lead to economic loss.

IT system

This can be defined as anything to do with a ship's computer's software, hardware, system, equipment and appliances, namely, Information Technology.



3－2 Explanation of Class NK technical information (No. TEC-1145)

Regarding IACS, the importance of security countermeasures of a computer system are to be considered. In order to specify the requirements related to a person's role in a computer system used on board, security countermeasures of both software and hardware to be used in the computer system and the quality of management, such as the procedure of software changes etc., the Unified Requirement of IACS E22(Rev.2) was adopted in June, 2016.

Following this, a notice of revised related rules and inspection procedures in the Class NK technical information

guideline (No. TEC-1145) was issued on February 28, 2018.

In the Class NK technical information guideline (No. TEC-1145), regarding each piece of software and hardware that performs automatic control or remote control installed on board, they were classified according to the extent of influence they exert by disorder. Further, responsibilities and duties were distinguished according to shipyard, system integrator, supplier and shipowner.

Table 2.1 System categories in Annex D18.1.1, Part D of the Guidance for the Survey and Construction for Steel Ships

Category	Effects Typical	system functionality
I	Those systems, failure of which will not lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.	- Monitoring function for informational or administrative tasks
II	Those systems, failure of which could eventually lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.	- Alarm and monitoring functions - Control functions which are necessary to maintain the vessel in its normal operational and habitable conditions
III	Those systems, failure of which could immediately lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.	- Control functions for maintaining the vessel's propulsion and steering - Vessel safety functions

(Quoted from No. TEC-1145)

Category III

System	Examples of detailed machinery and system
Main propulsion systems	Engine control system, Engine remote control system, Main boiler control system, CPP control system, Electric propulsion control system
Steering system control systems	Steering system, Azimuth thruster
Electric power systems	Generator engine control system, Electric power converter (for electric propulsion ship, etc.)
Safety systems	Fire detection and fighting system, Flooding detection and fighting system, Internal communication system, System involved in operation of life saving appliances equipment
Other systems	Dynamic positioning system, Drilling system

(Quoted from No. TEC-1145)

Category II

Liquid cargo transfer control systems	Cargo control system (e.g. cargo control console, cargo valve remote control system, cargo machinery emergency shut-down system), Reliquefaction system, Inert gas generator (including nitrogen generator), Oil discharge monitoring and control system
Fuel oil treatment systems	Viscosity control system, Fuel oil purifier
Stabilization and ride control systems	Fin stabilizer, Jetfoil
Alarm and monitoring systems for propulsion systems	Engine alarm and monitoring system (including data logger)
Other systems	Ballast transfer valve remote control system, Oily water separator, Oil content meter, Waste oil incinerator, Sewage treatment plant, Aux. boiler control system, Ballast water treatment system, SOx/NOx scrubber, NOx exhaust gas recirculation system

(Quoted from No. TEC-1145)

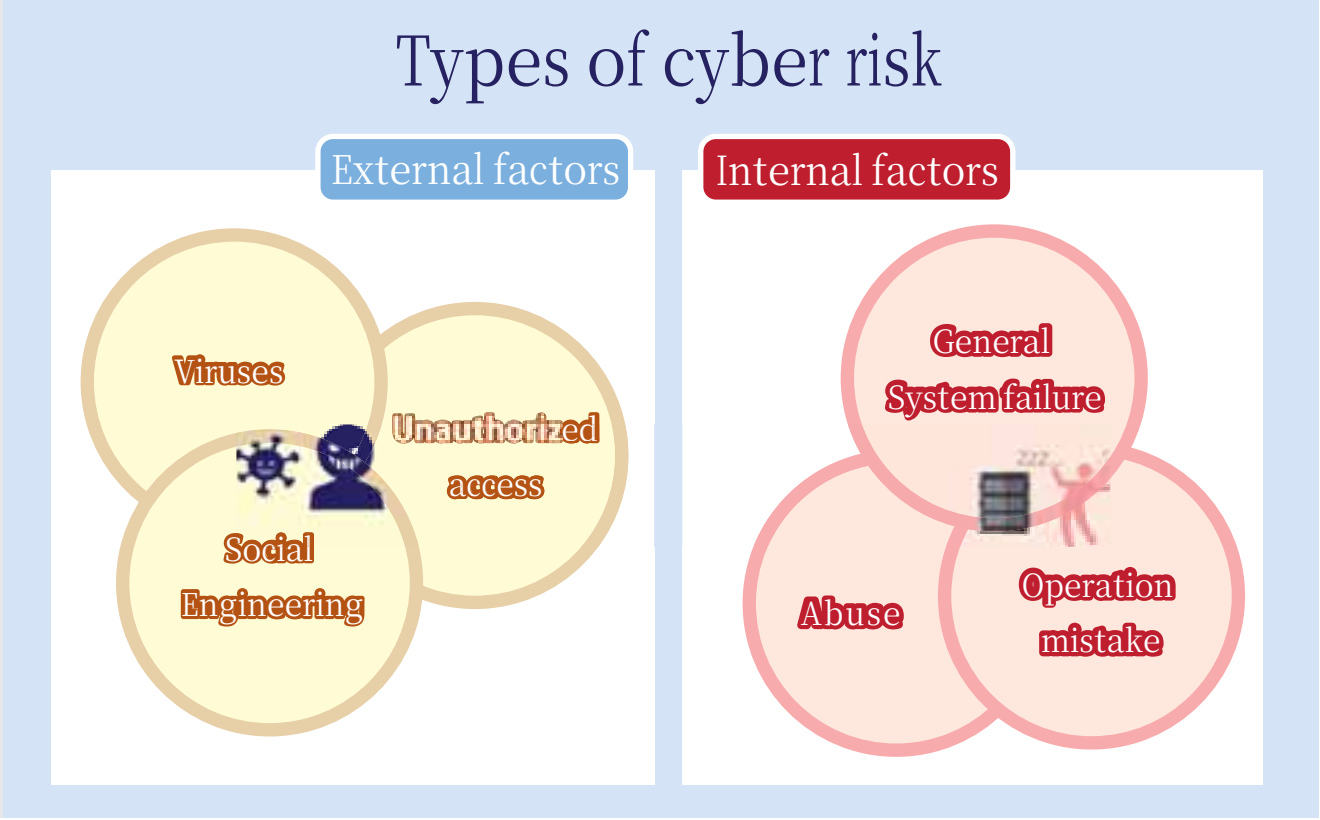
It is defined that the responsibility for cyber security countermeasures of each computer system is down to the supplier of each computer system. However, in the event of networking systems, the system integrator will be responsible because there will be new risks, which were not taken into account when operating a system as a single unit.

The role of the shipowner and ship management company is to keep receiving necessary information, such as a list of equipment that uses computers and risk assessment results etc. from the shipyard and system integrator; this is all that is required of them.

However, with respect to the revision of the SMS in the future (cyber security countermeasures), the concept “System integrator bears a certain amount of the responsibility” will play a key role. Regarding the onboard PC for duty use, loading computer, V-SAT, FBB and so on, which are classified into Class Category I, it will be necessary for a shipowner or ship management company to implement a risk assessment as a cyber security countermeasure.

3－3　Types of cyber risk

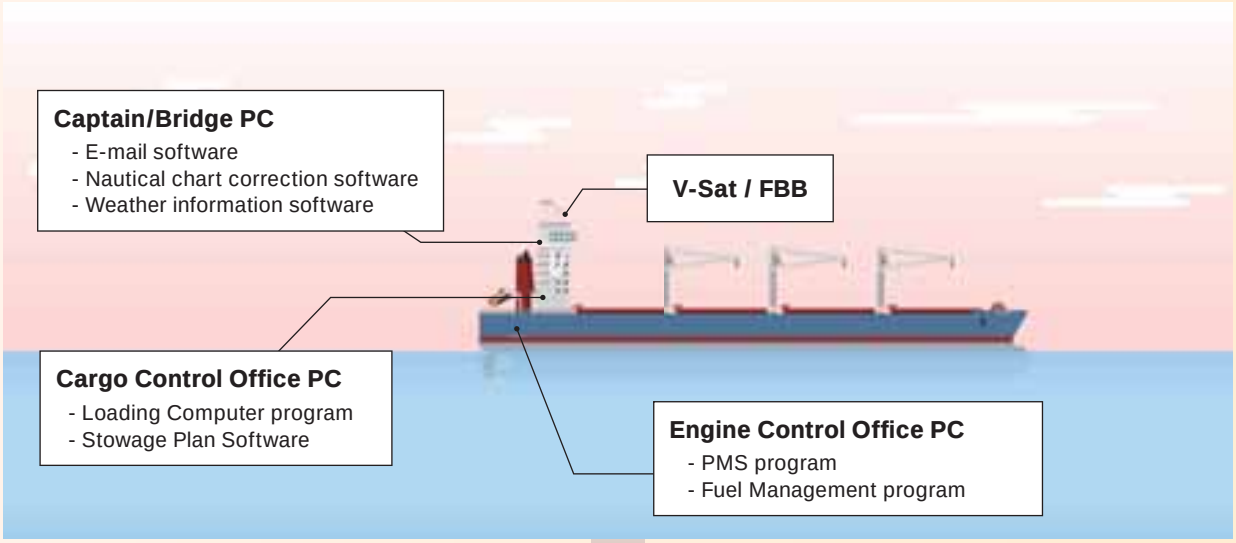
Although external factors such as unauthorized access and system hacking are mainly the focus when it comes to cyber risk, it will be important to consider reviewing internal factors, such as the existence of operation mistakes and general system failure.



3 — 4 How to make a plan for cyber security countermeasures

1 To identify the IT systems

After identifying the IT systems installed on the ship, list them up.



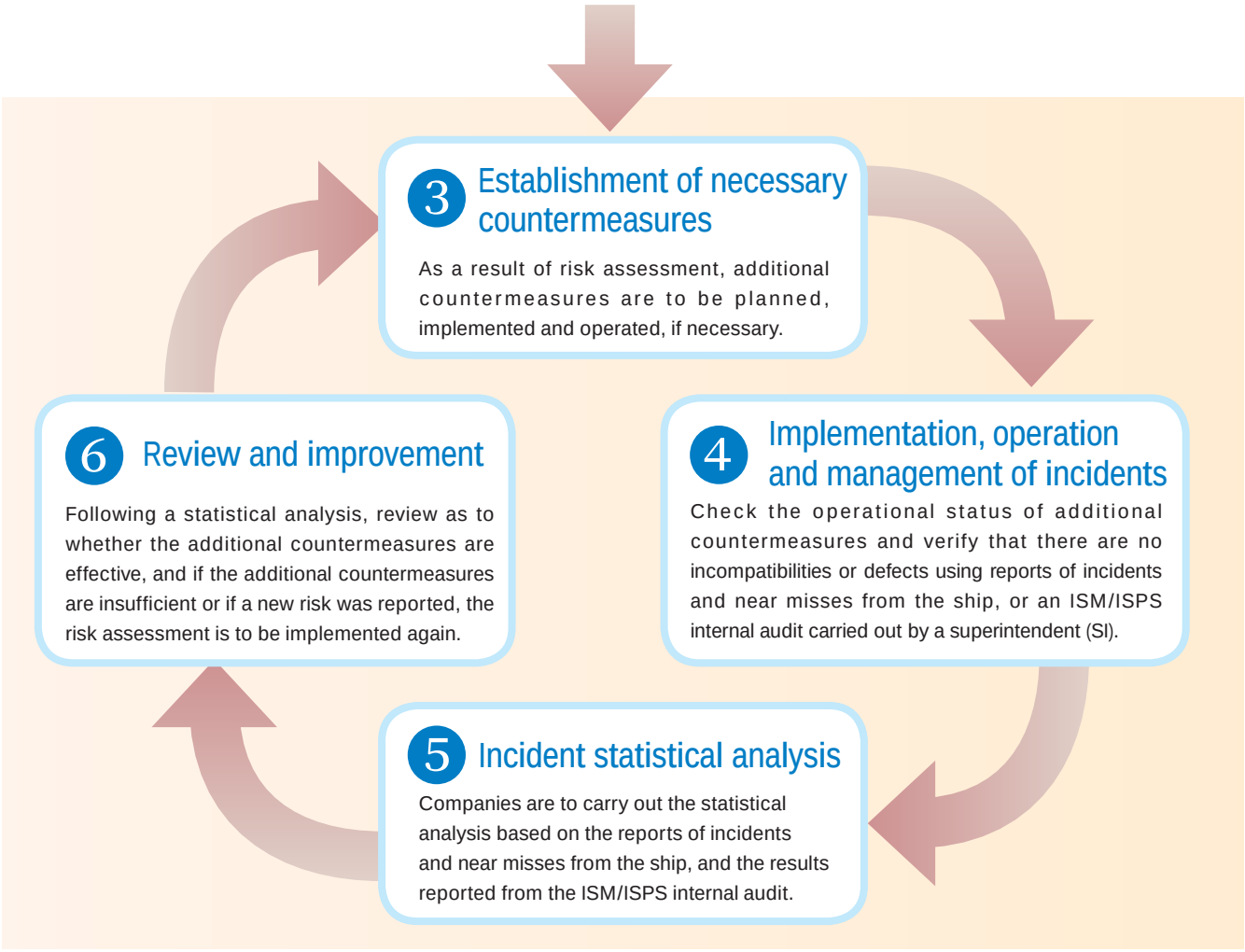
2 Implementation of risk assessment

For each listed-up IT system, risk assessment is to be implemented by examining the possible outcomes of a cyber attack (damage), frequency and current management method.

Table 4 Examples of risk assessment

E-mail communication							
No.	Scenario	Possibility	Frequency	Damage	Evaluation	Countermeasures	Due date
1	Malfunction of e-mail software infected by a virus from a crew member's personal USB	**Middle**	**Middle**	**Middle**	Additional countermeasure is required	① Additional SMS training ② Arrangement of a back-up PC	Dec., 2018
2	High cost of communications fee because firewall is not installed	**Middle**	**High**	**Middle**	Additional countermeasure is required	Dispatch a technician to the next port of call and install the FW and set up a filter in the FBB	Dec., 2018
3	Crew's personal PC that has been directly connected for the use of sending emails etc.	**Low**	**Low**	**Middle**	Risk tolerance	Although a certain amount of risk may be tolerated, this can be further mitigated by setting up the FBB filter	N/A
4	Malfunction of satellite and land earth station	**Low**	**Low**	**Middle**	Risk tolerance	N/A	N/A
5	Continued...						

The above is one example, because risk assessment and the SMS can differ depending on the crew structure, sea area for shipping operation, ship type and management company.



① ····· Identify the IT systems on the ship in order to list them up.

② ③ ··· In the same way that dangerous work and hazardous areas designated on the ship are operated using the current SMS, identify the onboard IT systems and implement a risk assessment while examining the possible outcome of a cyber attack (damage), frequency of and current management method, and carry out a countermeasure, if necessary. When confronted with a cyber risk, it is also necessary to consider trends in the IT field, types and versions of systems and equipment, and so on.

④ ····· Check the operational status of additional countermeasures and verify as to whether there were no incompatibilities or defects using reports of incidents and near misses from the ship, or an ISM internal audit carried out by a SI.

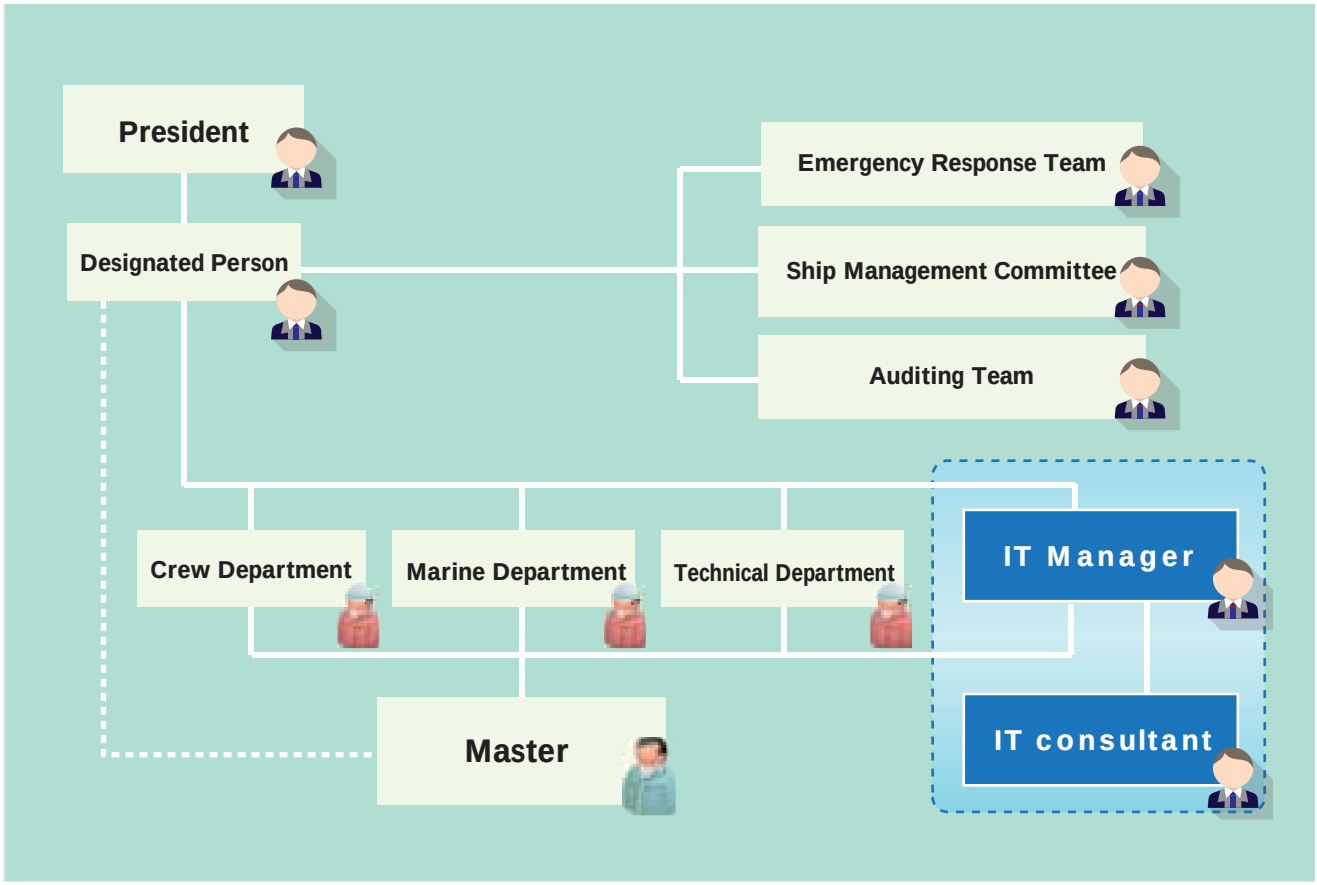
⑤ ⑥ ··· Companies are to implement the statistical analysis based on the reports of incidents and near misses from the ship, and the results reported from the ISM internal audit. Following the results of the statistical analysis, review (management review) as to whether the additional countermeasures were effective, and if the additional countermeasures were insufficient or if any new risks were reported, a risk assessment is to be implemented again, in the same way that the operation would be carried out with the existing SMS, and the necessary countermeasures are to be examined.

Regarding the reporting of incidents and near misses, the following examples can be said to be occurring recently: A crew member inserted a USB memory stick which is not permitted by the company, into their work PC, or he/she downloaded non-permitted software or a programme onto the onboard PC.

In addition, in order to receive visitors (external factors of cyber risk), not dissimilar to that of the SMS, it could be necessary to review the SSP, also, as an unspecified number of visitors and dock workers will get on board, especially at the port of call, and multi-purpose offshore support vessels and research vessels carrying a large number of researchers and workers may embark.

§4 Selecting designated IT personnel

We believe that it will be desirable to appoint an IT designated person when it comes to drawing up and implementing cyber security countermeasures that can be incorporated into the SMS. In the future, when countermeasures in a state of emergency and the introduction of systems maintenance on board a ship are required, the role of the IT Manager and the importance of this role will become more essential. In addition, it will be important to have a system in place that allows for consultation to be carried out with an external ship IT system expert.



§5 Establish an IT standard in your organization

The establishment of an IT standard will allow for the smooth integration of operation and management (maintenance etc.) if your organization is managing a large fleet of ships. With an IT standard in place, it will be much easier to deal with any problems that arise, compared to not having established one.

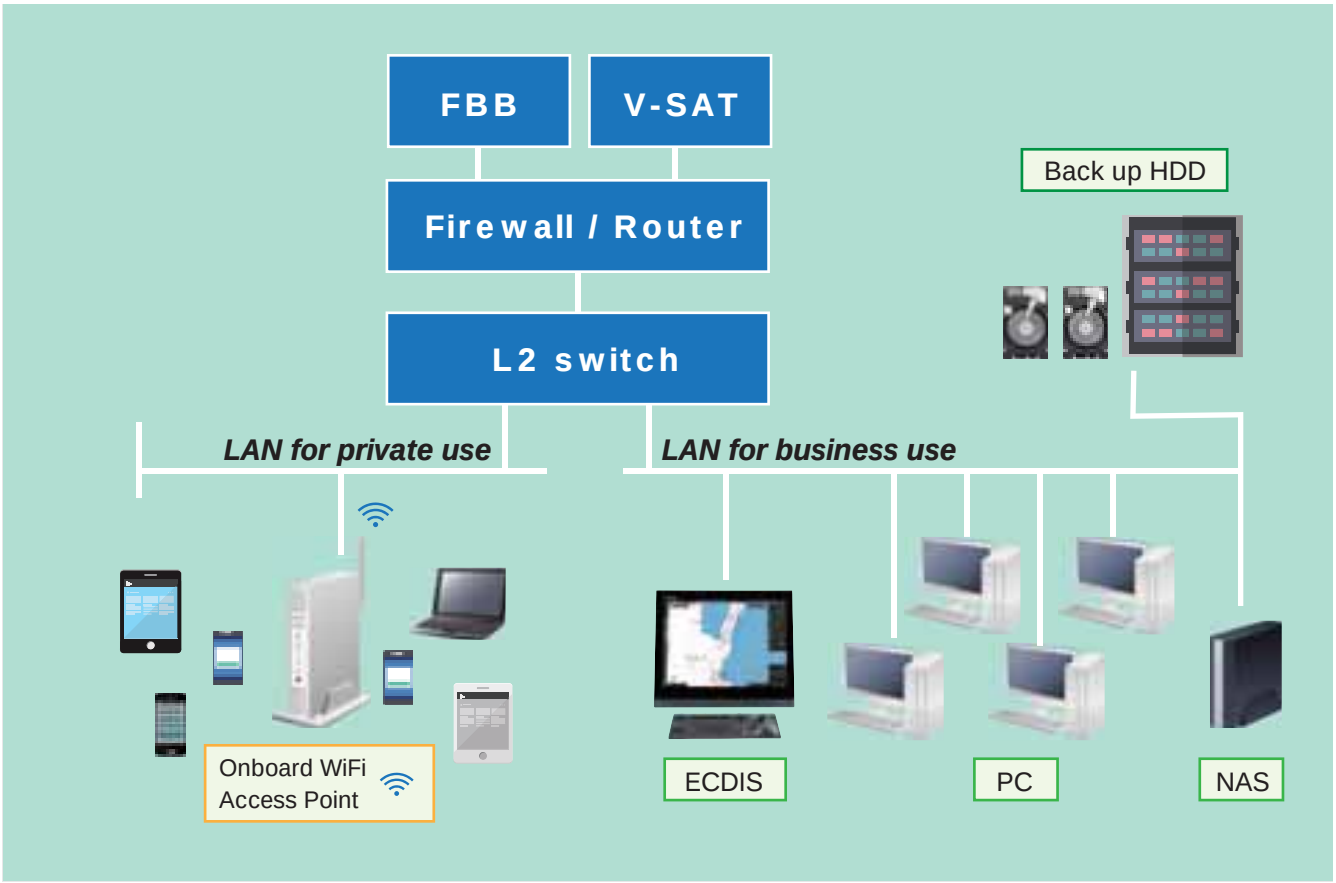


Fig. 5 Construction example of ship's LAN

It is important to organize the specification, software and purpose of each onboard PC. For reference, it will be useful if a substitute PC is available in case a PC breaks down or new software is added.

Record standard design of onboard PC!

Record for IT Standard Design

Standard type:
Date of Record:
IT Manager:
Designated Person:

This IT Standard will be value from :

I. Client PC Conditions				Remark
(1) Hardware				
	Number of PCs			
	Type (Laptop PC/Desktop PC)			
	CPU			
	Memory			
	HDD			
(2) Software	**Basic Software**			
	OS			
	MS-OFFICE (version)			
	MS-OFFICE (Applications)			
	Acrobat Reader			
	AntiVirus Software			
(3) Software	**Application Software**	**Applications**	**Suppliers**	
(4) Network Diagram	**Detail of PC setting**			
	Detail of PC setting	**(Refer to the second sheet)**		
II. Peripheral Device				
(1) Printer				
	Laser Printer			
	* Number of them			
	* Single or Multiple function			
	* Black/White or Color			
	Inkjet Printer			
	* Number of them			
	* Single or Multiple Function			
	* Black/White or Color			
(2) Scanner				
	* Number of them			
	* Flatbed/Stand			
(3) NAS set				
	* Model			
III. Network				
(1) Router				
	Type of Router			
	Supplier			
(2) Sub Network				
	Purpose of Sub Network			
(3) Wifi Access Point				
	Number of Wifi Access Point			
(4) Network Diagram				
	Network Diagram	**(Refer to the third sheet)**		

Table 6 Record for IT Standard Design

§6 Implementing an IT standard risk assessment

Regarding the IT standard (ship's LAN/onboard PC specification), risk assessment is to be implemented following the procedure that was established in the introduction of this guide “3-4 How to make a plan for cyber security countermeasures”.

Please note that systems that have already been risk assessed, IT systems that do not directly interfere with work being carried out even when a system failure occurs, stand-alone use computers etc. in Class Category II and III can be excluded from the risk assessment.

§7 SMS manual to include IT control documents

Having implemented a risk assessment and incorporation of the IT control documents into SMS manual, it is recommendable that a ship and shore joint drill that simulates a severe IT incident be implemented, even if only once. It would be a good opportunity to review as to whether the manual and instructions for cyber security countermeasures which were established in the SMS manual work effectively, and as to whether both personnel on shore and crew on the ship are familiar with the new manual and so on.

§8 Conclusion

It is hoped that if this Loss Prevention Bulletin will be put to good use and that it may assist you in your establishment of cyber security countermeasures.

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

Text and forms provided by ORCA CO., LTD.

Following test and forms are available on our Club website

Text and forms provided by ORCA CO., LTD.

Reference ICS Bridge Procedure Guide Fifth Edition