KR Maritime Cyber Safety

News from KOREAN REGISTER

Vol. 046

Feb 2022

[Special]

- Analysis of International Cyber Security Guideline : DCSA

- NIST Cybersecurity Framework five core elements

- 1.1 Asset Management

- 1.3 Governance

- 1.4 Risk Assessment

2.2 Awareness and Training

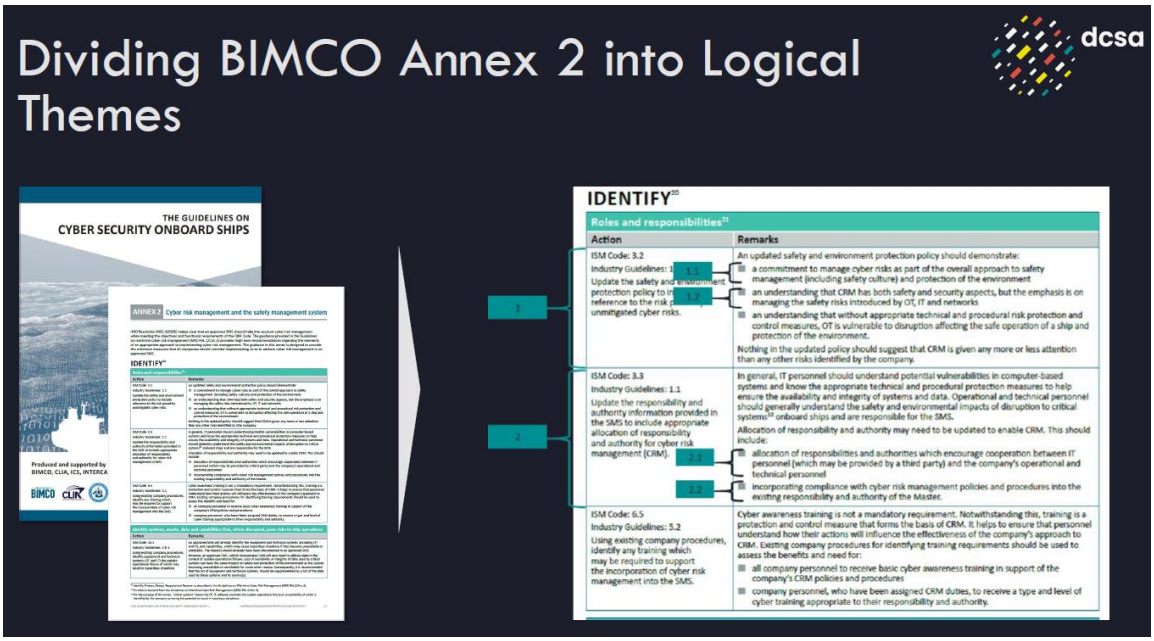
- 3.2 Security and Continuous Monitoring

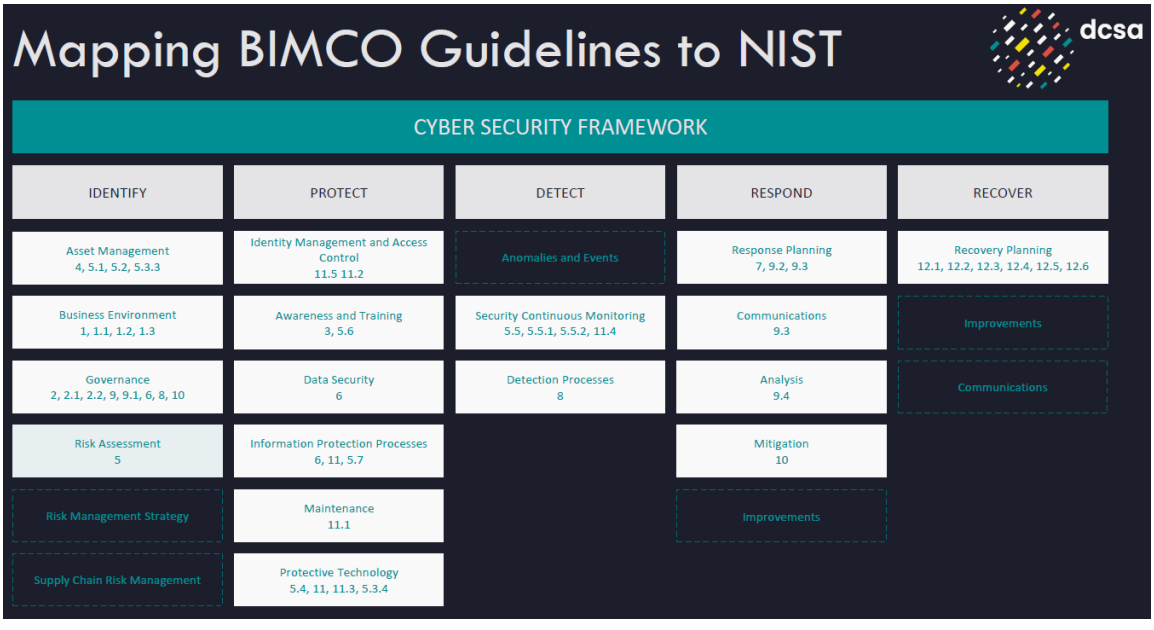
- 4.1 Respond Planning

- 5.1 Recover Planning

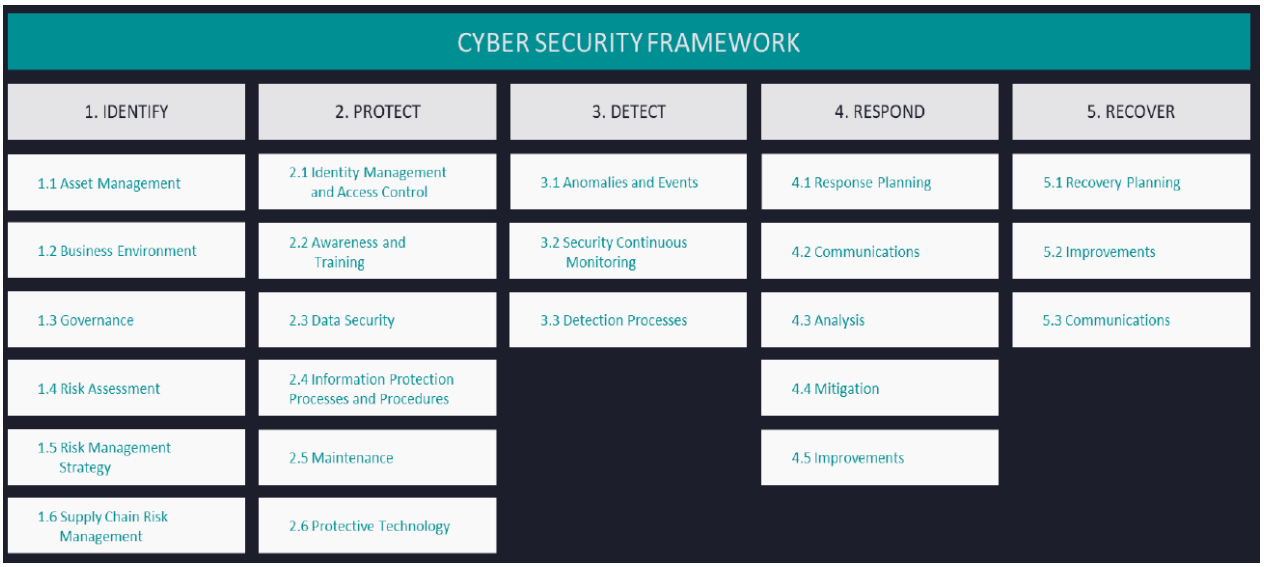
DCSA ship cyber security guideline objective

DCSA published implementation guide for cyber security on vessels in 2020. This guideline maps the cyber considerations specified in the BIMCO Ship Cyber security Guidelines for response to IMO MSC.428(98) Resolution with the NIST Cybersecurity Framework (IDENTIFY-PROTECT-DETECT-RESPOND-RECOVER). It also provides guidelines on how to implement each requirement by providing explanations and examples.





NIST Cybersecurity framework five core elements



1. IDENTIFY – Develop an organizational understanding for managing cyber security risks to systems, assets, data and functions. Understanding the business context, the resources supporting its core functions, and the associated cyber security risks can help organizations focus and prioritize their efforts to align risk management strategies and business requirements.

2. PROTECT - Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services. Protection functions support the ability to limit or contain the impact of potential cyber security incidents.

3.DETECT - Develop and implement appropriate activities to detect the occurrence of cyber security incidents. Detection capabilities enable timely discovery of cyber security incidents.

4.RESPOND - Develop and implement appropriate activities to take action on detected cyber security incidents. Response capabilities support the ability to contain the impact of potential cyber security incidents.

5.RECOVER - Maintain a resilient plan and develop and implement appropriate activities to recover a function or service that has failed due to a cybersecurity issue. The recovery function supports timely recovery to work normally to reduce the impact of a cybersecurity incident.

1.1 Asset Management

NIST cybersecurity framework specifies six requirements (ID.AM-1 ~ ID.AM.6) for asset management (1.1).

- **BIMCO (5.1) : Ensure that all critical hardware devices within the vessel are inventoried**
- **BIMCO (5.2.2) : Ensure there is a maintenance procedure for this inventory when company-managed software is updated or changed**

BIMCO	NIST	NIST CONTROLS - SP 800-53 REV. 4
• 4 • 5.1 • 5.2 • 5.3.3	ID.AM-1: Physical devices and systems within the organisation are inventoried.	CM-8, PM-5
	ID.AM-2: Software platforms and applications within the organisation are inventoried.	CM-8, PM-5
	ID.AM-3: organisational communication and data flows are mapped.	AC-4, CA-3, CA-9, PL-8
	ID.AM-4: External information systems are catalogued.	AC-20, SA-9
	ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.	CP-2, RA-2, SA-14, SC-6
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.	CP-2, PS-7, PM-1

Necessity of Asset Management

A ship can be considered from a cybersecurity point of view as a 'system' operating in an isolated environment with an external communication interface. The size and complexity of this system will depend on the size of the vessel, and to effectively manage cyber risk, it is necessary to fully identify what assets are on the vessel. IT/OT systems that need to be managed for cyber security may be in or related to the following categories:

System	Explanation
Communication	Systems provided for internal, ship-to-ship communication.
Navigation	Systems provided for vessel navigation
Plant	Monitoring of machinery and plants related to the operation of ships system used to control
Cargo	Systems used to directly monitor and manage cargo
Crew Access	Systems provided for seafarers

Asset inventory (sample)

Before planning and conducting risk assessments, the assets in the organization must first be identified. The best way is to inventory assets. The asset inventory must include all assets of value to the organization and contribute to its function. This includes physical devices, systems, software platforms and applications, and should include the following.

dcsa	Asset List							
	Example asset list which can be populated with a list of critical assets including type (hardware/software), owner (shore), custodian (on vessel) and criticality based on existing impact assessments within the SMS.							
Asset Serial	**Asset**	**Type/Description**	**Version**	**Owner**	**Custodian**	**Location**	**Date of Last Check**	**Criticality**
1	Dell Inspiron 17 Laptop	Hardware	Windows 10	J Doe	A Smith	Bridge	01/11/2019	Low
2								
3								
4								
5								
6								
7								
8								
9								
10								

- Serial number
- Asset type (hardware/software)
- Asset name
- Asset owner
- Version number
- Location
- Date of last review
- Criticality (low, medium, high, safety critical)

This should form part of an asset lifecycle management process which documents the procurement or creation, processing, storage, transmission, deletion and destruction activities. This lifecycle should be documented in an asset register.

Asset Criticality criteria

Measuring Weight of an asset (criticality)		
Weight	**Rate**	**Description**
Low	1	The asset value is low based on low business objectives, and would have little / no critical impact to the organisation if the asset was lost or damaged
Medium	2	The asset value is medium based on business objectives, and would have some critical impact to the organisation if the asset was lost or damaged
High	3	The asset value is high based on business objectives, and would have high critical impact to the organisation if the asset was lost or damaged

1.3 Governance

The ship is establishing governance to achieve the business environment goal of ensuring safety and continuation of operation. For cyber security onboard ships, additional governance (cyber security roles and responsibilities) should be considered as appropriate for the size of the company/vessel. There should be defined roles and personnel with cybersecurity responsibilities on board, and the company should establish appropriate governance regarding the roles and responsibilities of CSOs and CySOs and ensure that they are integrated into the existing governance structure.

NIST cybersecurity framework specifies four requirements (ID.GV-1 ~ ID.GV.4) related to governance (1.3).

BIMCO	NIST	NIST CONTROLS - SP 800-53 REV. 4
• 2 • 2.1 • 2.2 • 6 • 8 • 9 • 9.1 • 10	ID.GV-1: organisational cybersecurity policy is established and communicated.	-1 controls from all security control families
	ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.	PS-7, PM-1, PM-2
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy.	-1 controls from all security control families
	ID.GV-4: Governance and risk management processes address cybersecurity risks.	SA-2, PM-3, PM-7, PM-9, PM-10, PM-11

Designated Person Ashore (DPA)

The DPA will under normal circumstances be the Cyber Security Lead officer of a carrier and will cooperate with the CISO. They are responsible for implementing and maintaining the Cyber Security Framework fleetwide and will have functional responsibility for Cyber Security roles on-board vessels.

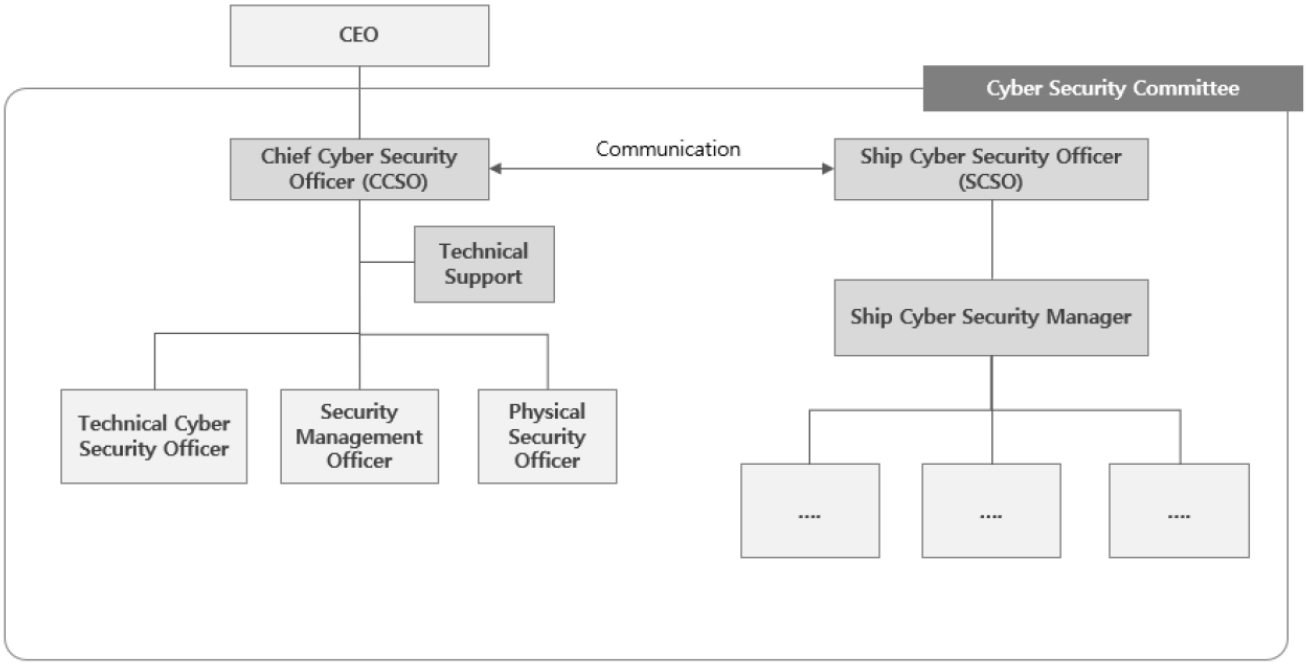
- Develop and manage a cyber security program that follows BIMCO as an industry standard
- Facilitate communication with the senior management
- Mediate disputes related to policies and standards

Cyber Security Officer (CySO)

The CySO is responsible for all security aspects of cyber-enabled systems on the ship, including the IT, OT and communications systems.

- Coordinating with the Company security officer (CSO) on aspects relating to physical, personnel and process security; and
- Ensuring the development, periodic review and maintenance of the CSA/CSP; and
- Implementing and exercising the CSP .

Cyber security organization chart (sample)



Chief Cyber Security Officer (CCSO) R&R (sample)

Retain qualification
1. Cyber security professional training **(4 hours/year)**
Cyber Security Role and Responsibility
1. Final decision maker and director
2. Review and approve cyber security regulations (policies, manuals, procedures)
3. Review and approve Cyber security action plan
4. Communicate and report to CEO, communicate with Technical Cyber Security Officer, SSO
5. Coordination of security issues between organizations and improvement of security management process
6. Security external contacts
7. (Ship and company) Cyber security policy establishment and management System
8. Establishment of cyber security incident response management system and follow-up
9. (Ship and company) Cyber security education and change management
10. (Ship and company) Periodic / occasional security management level check request and consultation
11. Organizing cyber security team

1.4 Risk Assessment

Risk assessment is one of the most important activities of cyber security to eliminate a company's business goals, asset importance, and asset threats and vulnerabilities. Potential cyber threats should already be identified in the Safety Management System Risk Library (SSA) and mitigated through SSP, and the impact of these threats on the cyber security of ships and ship systems should be understood.

NIST cybersecurity framework specifies four requirements (ID.RA-1 ~ ID.RA.6) related to risk assessment (1.4).

BIMCO	NIST	NIST CONTROLS - SP 800-53 REV. 4
• 5	ID.RA-1: Asset vulnerabilities are identified and documented.	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
	ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources.	SI-5, PM-15, PM-16
	ID.RA-3: Threats, both internal and external, are identified and documented.	RA-3, SI-5, PM-12, PM-16
	ID.RA-4: Potential business impacts and likelihoods are identified.	RA-2, RA-3, SA-14, PM-9, PM-11
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	RA-2, RA-3, PM-16
	ID.RA-6: Risk responses are identified and prioritized.	PM-4, PM-9

Risk Assessment process

1. Context establishment : Determine asset range, metric, threat vulnerability list, governance model, etc.

2. Risk analysis

1) Determining whether a threat can exploit a vulnerability within a specified asset.

2) Allocate scores to each identified risk using a risk matrix

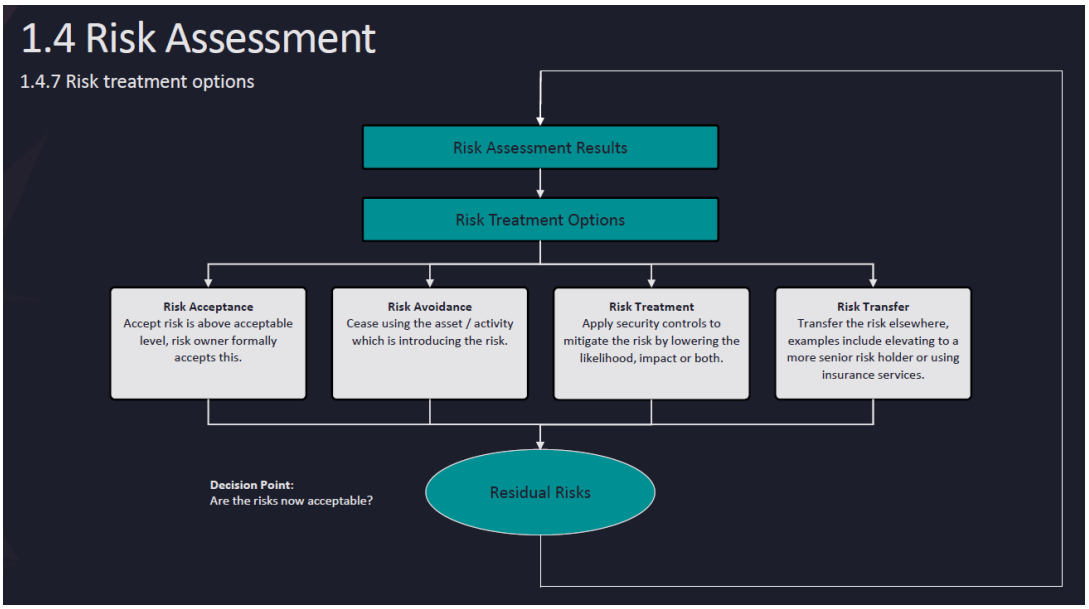
3) Determining a risk response strategy (acceptance, reduction, avoidance, transfer)

3. Risk management: Establishing a risk management plan on what controls (management, physical, and technical controls) can be performed to mitigate risk ratings. Determining the implementation and operation costs

4. Risk monitoring : Establishing a process to monitor risk control effectiveness to identify improvements

Risk Treatment Strategy

- **Risk acceptance** : Accept current risks and bear the cost of potential losses.
- **Risk avoidance** : Giving up without carrying out a risky process or business
- **Risk treatment** : Adopt and implement measures that can reduce risk, and conduct cost-effectiveness analysis
- **Risk transfer** : transferring or allocating potential costs to a third party through insurance or outsourcing



Risk Assessment Terminology

Terminology	Explanation
level of risk	Size of risk (combination of likelihood and impact)
residual risk	Risk remaining after action
risk analysis	The process of identifying risks to determine risk
risk assessment	Process covering risk identification, risk analysis, and risk level evaluation
risk criteria	Criteria for judging the importance of risk.
risk evaluation	In order to determine whether to accept risk, the procedure for comparing the risk analysis results with risk criteria.
risk identification	Procedures for identifying risk
risk management	Activities to control risk

Risk Calculation

Risk can be calculated as Severity x Probability. A score of 5 for both Severity and Probability negatively impacts the organization. Therefore, it is important to define what level of risk is to be accepted. If the risk acceptance criteria is set to '16', all risks above '16' should be mitigated.

	Severity			Likelihood	
5	Catastrophic	Severe impact to the organisation. Loss of resources and worst case loss of life	5	Almost certain	A threat is very likely to occur. Could be multiple times per week
4	Major	Serious impact to the organisation. Will damage both reputation and compromise of information	4	Likely	Two to three times per month
3	Moderate	Partially damaged image and loss of costumer confidence. Some negative impact to the organisation and its operation	3	Possible	Occurs once per month
2	Minor	Small harm to the organisation.	2	Unlikely	Occurs once or twice a year
1	Negligible	Insignificant impact to organisation and operations.	1	Rare	Few previous incidents: happens once every 10th year

Catastrophic	5	10	15	20	25
Major	4	8	12	16	20
Moderate	3	6	9	12	15
Minor	2	4	6	8	10
Negligible	1	2	3	4	5
	Rare	*Unlikely*	*Possible*	*Likely*	*Almost certain*

System	Impact	Likelihood	Initial risk	Mitigation	Residual risk
ECDIS	**Score 5** due to risk of catastrophic events like grounding and collision	**Score 4** due to active USB ports, computer used for other purposes, connection to admin network for access to shared printer, connection to automatic chart updates via satellite via trusted vendor	Risk = 5 x 4 = 20	Password protect and restrict PC use to ECDIS only	Risk = 5 x 3 = 15
				Disconnect from admin network	Risk = 5 x 2 = 10
				Blind off USB ports	Risk = 5 x 1 = 5

Source : BIMCO Guidelines on cyber security onboard ship(Ver.4)

Apply CIAS to Risk Assessment

CIAS index stands for confidentiality, integrity, availability and safety, and can be used for risk assessment.

- **Confidentiality** : ability to protect data, so that only those users with appropriate permission levels are authorised to view data. It could also assess the protections to be applied to data classified as confidential. This can be ensured by using Access Control Lists
- **Integrity** : reliability of data stored recorded by and stored within an organisation. If there is a high risk of data being altered during an incident, the score for integrity will be high. Data encryption or hashing are useful tools to ensure a high level of integrity.
- **Availability** : lack of availability of systems. If an incident were to occur, where the systems would be down for 15 minutes, the availability score would be 1. Redundancy or RAID can be used to mitigate incidents from happening5.
- **Safety** : It is also important to incorporate in the risk assessment, as it focuses on people. If the score is 1, there is a hazard identified, but no one's safety is at risk. If the score is at 5, which is the worst case scenario, an incident would have led to loss of life.

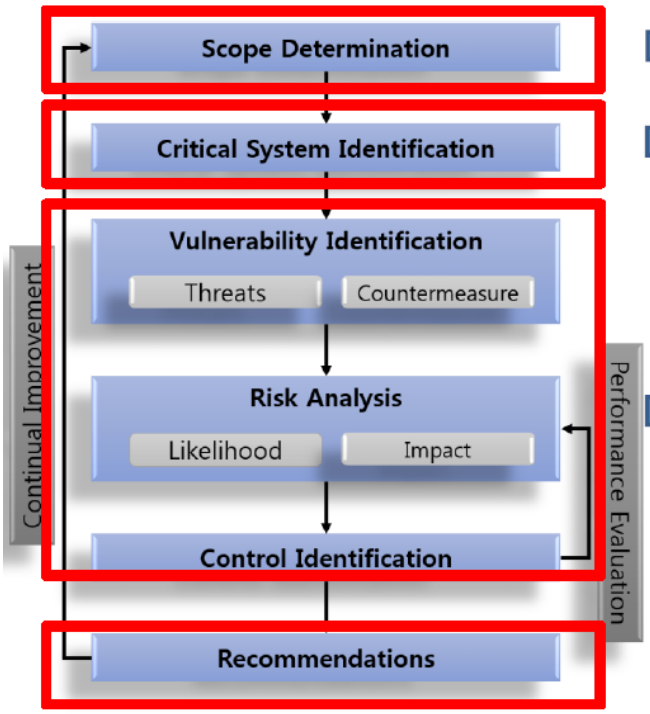
	Confidentiality	Integrity	Availability	Safety
1	Negligible	No noticeable change	15min	Hazard identified
2	PD/IP	Smaller change, data or system still usable.	1 hour	Hazard occurs, but no injury (near miss)
3	Data breach	Noticeable change, diminishes usability of data or system.	6 hour	Minor injury – requires treatment but able to continue working.
4	Large data breach	Significant changes to data or settings, requires significant effort to recover.	One day	Major injury – unable to continue working/evacuation from ship.
5	Data breach detrimental to the organisation	Data or settings are fatally corrupted.	One week	Loss of life.

If no controls are available to mitigate the risk (malware), the CIA score is 5 and the impact score is 25 (severity x likelihood). If control (eg antivirus) measures are in place to mitigate the risk, the CIA score is expected to be lower than 5, so it is reduced to an impact score (15).

Risk description	Inherent Impact / Risk category				Likelihood	Impact score
	C	I	A	S		
Malware propagation	5	5	5	3	5	25

Control(s)	Risk description	Residual risk Impact / Risk category				Likelihood	Impact score
		C	I	A	S		
Antivirus	Malware propagation	3	3	3	3	5	15

KR Cyber Security Risk Assessment Process



Step 1 Scope Determination

Network Topology, Asset List, etc.

Step 2 Critical System Identification

Criticality Index (CrI) = Confidentiality Index (CoI)
+ Integrity Index (II)
+ Availability Index (AI)

Step 3 Cyber security Risk Assessment

3-1 Threat & Vulnerability
3-2 Risk Analysis
3-3 Control Identification

Risk Index (RI) = Threat Index(TI) x
Vulnerability Index(VI) x CrI

Step 4 Recommendations

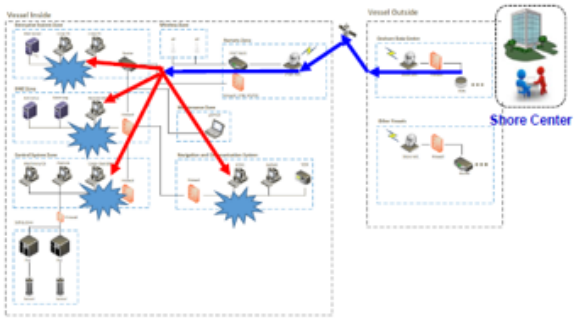
Identify cyber threat

No. (old No.)	Top 10 2016	Top 10 2014
1 (3)	Social Engineering and Phishing*	Malware Infection via Internet and Intranet
2 (2)	Infiltration of Malware via Removable Media and External Hardware	Infiltration of Malware via Removable Media and External Hardware
3 (1)	Malware Infection via Internet and Intranet	Social Engineering
4 (5)	Intrusion via Remote Access	Human Error and Sabotage
5 (4)	Human Error and Sabotage	Intrusion via Remote Access
6 (6)	Control Components Connected to the Internet	Control Components Connected to the Internet
7 (7)	Technical Malfunctions and Force Majeure	Technical Malfunctions and Force Majeure
8 (9)	Compromising of Extranet and Cloud Components	Compromising of Smartphones in the Production Environment
9 (10)	(D)DoS Attacks	Compromising of Extranet and Cloud Components
10 (8)	Compromising of Smartphones in the Production Environment	(D)DoS Attacks

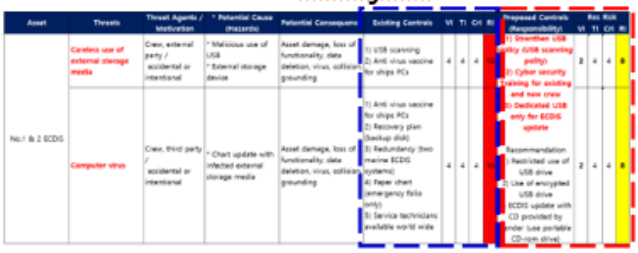
Ref. : BSI Industrial Control System Security – Top 10 Threats and Countermeasures 2016

Identify cyber attack scenario

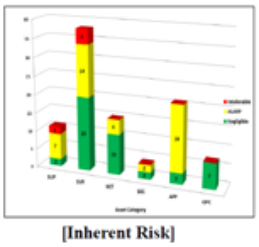
Threat	Cause	Agent	Consequence
Malware	Remote update and maintenance	External	System malfunction / network infection



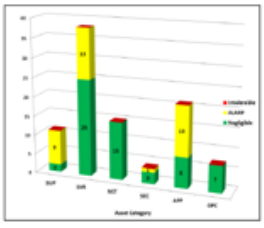
Risk Anlaysis



Risk Score



[Inherent Risk]



[Residual Risk]

2.2 Awareness and Training

People are the most vulnerable factor in cyber security. It lowers the overall security level of companies/vessels by clicking malicious links in emails, executing malicious files, transferring malicious files to the system or environment through USB, and using weak passwords. Therefore, the company/ship must determine appropriate security awareness education and training content.

NIST cyber security framework specifies five requirements (PR.AT-1 ~ PR.AT-5) related to awareness and training (2.2).

BIMCO	NIST	NIST CONTROLS - SP 800-53 REV. 4
• 3 • 5.6	PR.AT-1: All users are informed and trained	AT-2, PM-13
	PR.AT-2: Privileged users understand their roles and responsibilities	AT-3, PM-13
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	PS-7, SA-9, SA-16
	PR.AT-4: Senior executives understand their roles and responsibilities	AT-3, PM-13
	PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	AT-3, IR-2, PM-13

There should be a formal process to define the training and awareness requirements for crew members on-board vessels. It may be worth conducting audience segmentation, where different groups with different anticipated exposure levels to IT and OT assets have different training and awareness curriculums. An example of this could be:

- Group 1 – Specialists with dedicated information security roles, such as Incident Responders or roles that hold administrator level access. Any seafarer who has designated security duties shall undertake approved security training meeting the requirements of Table A-VI/6-2 of the STCW (International Convention on Standards of Training, Certification and Watchkeeping for Seafarers)
- Group 2 – Generalists with user access to critical systems. All seafarers must receive approved security awareness training or instruction that can be conducted on-board ship or ashore. This is not ship-specific and only has to be completed once.
- Group 3 – All other crew. All people employed or engaged on a seagoing ship must receive security-related familiarization training conducted by the Ship Security Officer or other equally qualified person.

Cyber security awareness poster (sample)

CYBER SECURITY ONBOARD SHIPS

Cyber security is everybody's responsibility.
The information provided here gives advice on how your actions can help to avoid cyber incidents.

POTENTIAL THREATS

KEEP UNAUTHORISED SOFTWARE AWAY FROM SHIP SYSTEMS!

- Scan for viruses and malware before you connect authorised USB memory sticks to onboard OT and other networked systems.
- Personal laptops, tablets, USB memory sticks or phones must not be connected to onboard operational systems.

INCIDENTS

BE PREPARED!

- Keep your crew and any passengers safe – train for what to do if important OT systems do not work.
- Know where to get IT and OT assistance.
- Report suspicious or unusual problems experienced on IT and OT systems.

PASSWORD PROTECTION

BE IN CONTROL!

- Use new passwords every time you sign on to a ship.
- Choose complex passwords with num6er5s, $ymbo!s, and some CaPiTaL letters. Be careful, you have to be able to remember them.
- Keep your user names and passwords to yourself.
- Change default user passwords and delete user accounts of colleagues who have left the ship.

SUSPICIOUS ACTIVITY

BE VIGILANT WHEN YOU COMMUNICATE!

- Only open emails or open attachments from senders that you know and trust.
- Know what to do with suspicious emails.
- Think before you share information on social media or personal email about your company, job, ship or the crew.

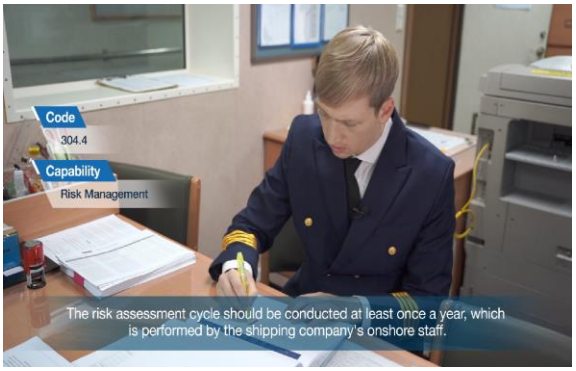
INTERNATIONAL CHAMBER OF SHIPPING · BIMCO · MPA SINGAPORE

OT: Operational Technology is the systems which are used to operate the ship.

IT: Information Technology is the systems used for office work, email and web-browsing.

KR cyber security e-learning

KR cyber security training material

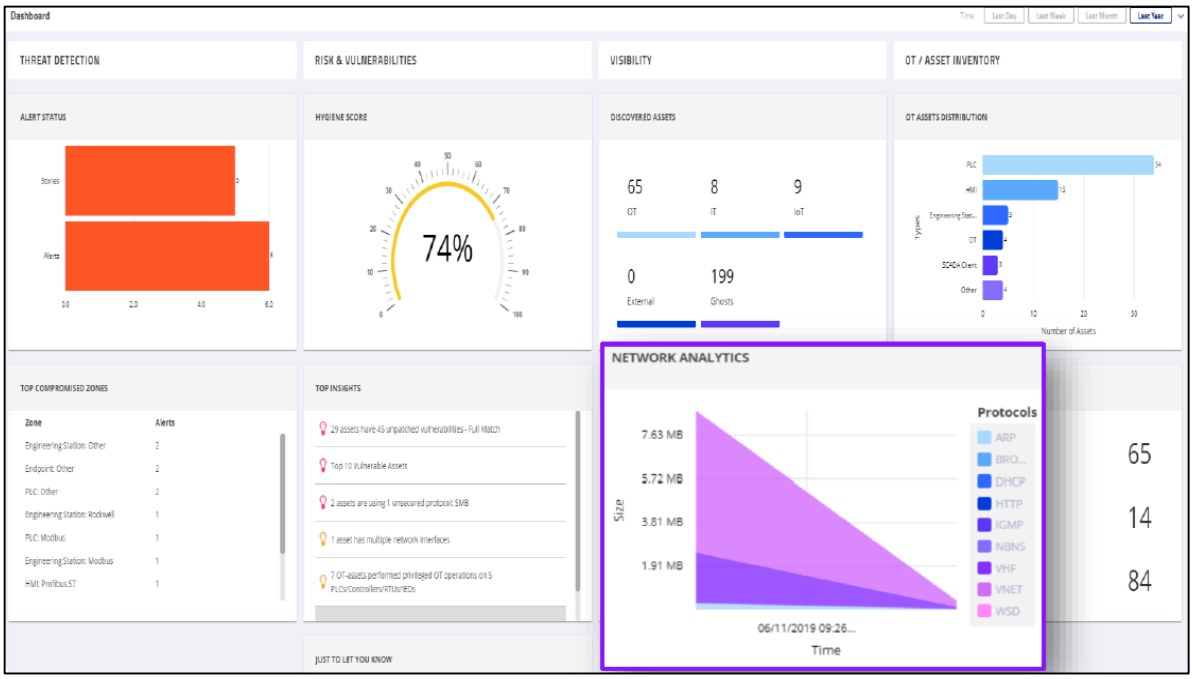


3.2 Security and Continuous Monitoring

Security and continuous monitoring can take the form of a number different capabilities such as monitoring event logs from critical assets and network devices using a Security Information and Event Management (SIEM) platform tuned to trigger alerts in the event of insecure or malicious activity on systems. Another option is to periodically review settings and configurations of assets to ensure that they are in the correct state and that there haven't been malicious or accidental changes.

NIST Cybersecurity Framework specifies eight requirements (DE.CM-1 to DE.CM-8) related to security and continuous monitoring (3.2).

BIMCO	NIST	NIST CONTROLS - SP 800-53 REV. 4
• 5.5 • 5.5.1 • 5.5.2 • 11.4	DE.CM-1: The network is monitored to detect potential cybersecurity events	AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	CA-7, PE-3, PE-6, PE-20
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
	DE.CM-4: Malicious code is detected	SI-3, SI-8
	DE.CM-5: Unauthorised mobile code is detected	SC-18, SI-4, SC-44
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	CA-7, PS-7, SA-4, SA-9, SI-4
	DE.CM-7: Monitoring for unauthorised personnel, connections, devices, and software is performed	AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
	DE.CM-8: Vulnerability scans are performed	RA-5



4.1 Response Planning

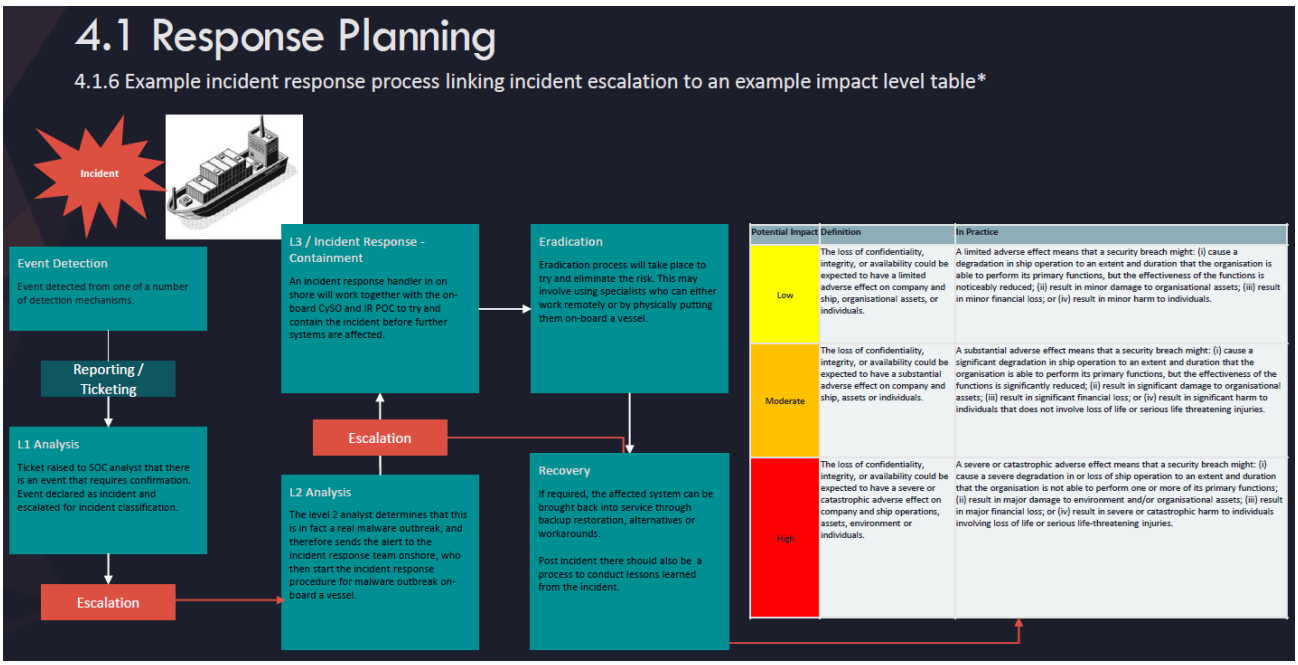
A Security Incident Response plan ensures that each cyber incident is reported, investigated, contained and remediated. In the event of a security incident it is vital, from both a business and a safety perspective, that a ship is able to operate without disruption or compromise of on-board essential systems.

The NIST cybersecurity framework specifies one requirement (RS.RP-1) related to the response plan (4.1).

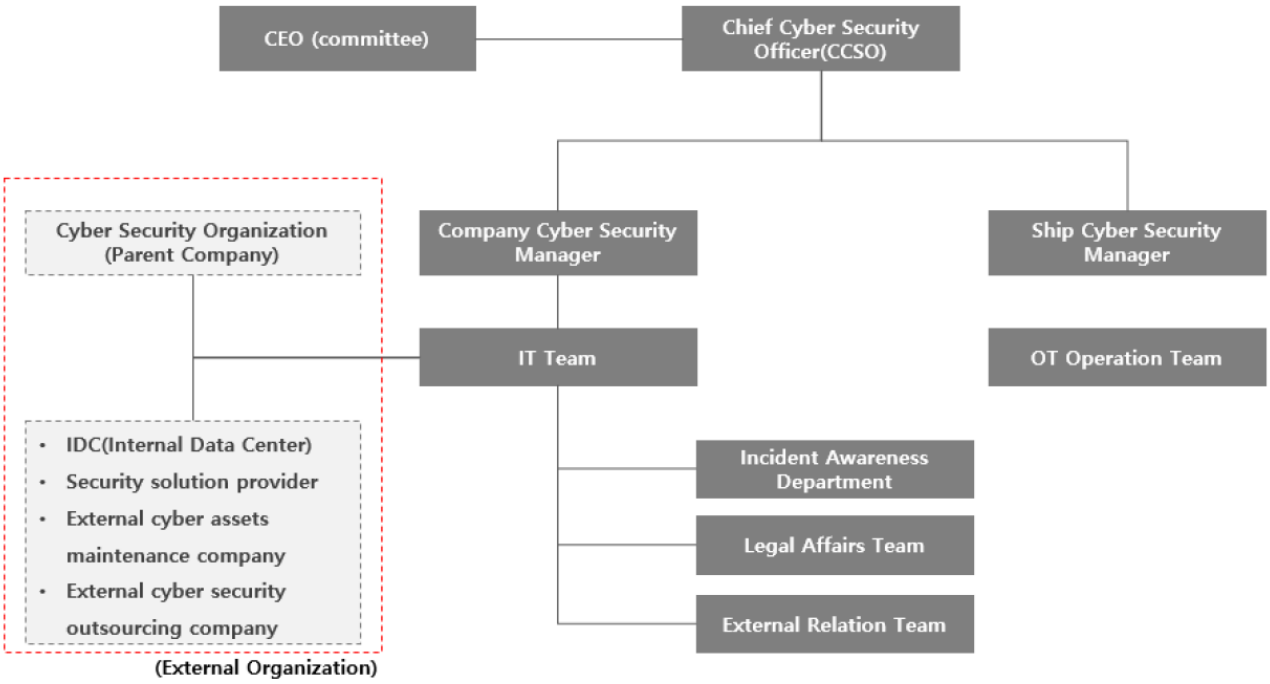
BIMCO	NIST	NIST CONTROLS - SP 800-53 REV. 4
• 7 • 9.2 • 9.3	RS.RP-1: Response plan is executed during or after an incident	CP-2, CP-10, IR-4, IR-8

A vessel should have in place a Security Incident Management Plan which is based on :

- Procedures for both incident response plans and preparation
- A process that initiates on the detection of an incident
- Clear communications guidelines for crew, covering reporting lines on-board the vessel and back to company headquarters ashore.
- A process to record incident response steps and activities
- A process for handling forensic evidence is in place

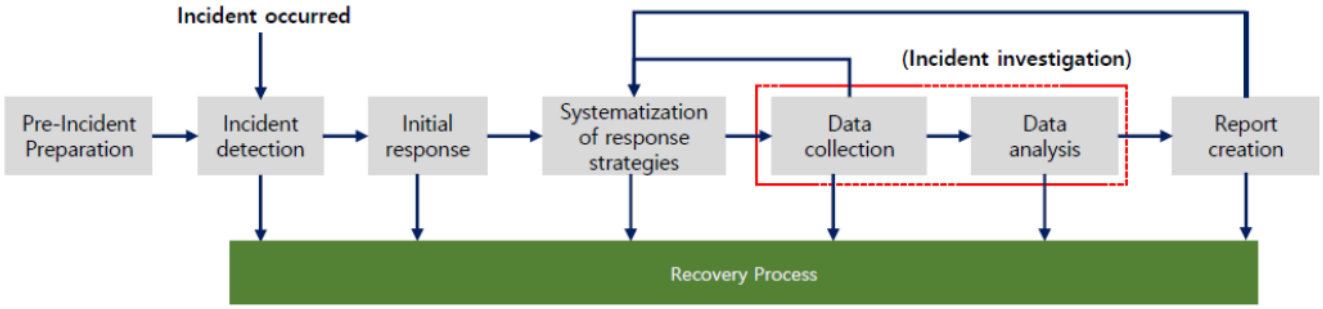


Cyber security response team and R&R(sample)



Department	Tasks
Cyber Security Team	• General management of company or ship cyber security incident response • Report on the cause of the incident, progress, follow-up status • Operation of emergency contact network and instructions • Announce measures to prevent incident in the organization • Analysis of causes of incident and preparation of countermeasures • Internal help-desk Operations
IT Team and OT Operation Team	• Analysis of cause of incident system or preservation of evidence • Emergency system operation or system emergency recovery • Data recovery and operation • Review cyber security solutions and apply follow-up measures
Incident awareness department (Company & Ship)	• Incident recognition and internal reporting • Write details about security incidents when reporting
Legal Affairs Team	• Consultation on related supervisory agencies due to incident • Report an incident or emergency incident • Consult with cyber security team to minimize legal issues
External Specialist	• Emergency recovery and restart of related systems through IDC, security solution operators, and system maintenance company

Cyber security incident response procedure(sample)



Level	Details
Pre-Incident Preparation	Prepare an incident response team and systematic response before an incident
Incident detection	Information protection and detection of abnormal signs by network equipment. Identification of cyber incident by administrator
Initial response	Perform initial investigations, record basic details of the incident situation, notification of incident response team, call to invasion incident department
Systematization of response strategies	Determine optimal strategy and obtain administrator approval. Judge whether or not the investigating agency is cooperating with the incident investigation process
Incident investigation	Data collection and analysis. Determine when, who, how an incident occurred, how to prevent the spread of damage and recurrence of incident
Report creation	Accurate reporting of incidents in a format that decision makers can easily understand
Recovery and resolution	Establish a security policy to identify and prevent future similar attacks, change procedures, record incidents, establish long-term security policies, and establish technology correction plans

5.1 Recovery Planning

Resilience is the ability to adapt, respond and recover rapidly from disruptions and maintain continuity of business operations. In the event of an incident it is vital, from both a business and safety perspective, that a vessel is able to operate without disruption or compromise of the services provided to its crew and users.

NIST Cybersecurity Framework specifies one requirement (RC.RP-1) related to the recovery planning (5.1).

BIMCO	NIST	NIST CONTROLS - SP 800-53 REV. 4
• 12.1 • 12.2 • 12.3 • 12.4 • 12.5 • 12.6	RC.RP-1: Recovery plan is executed during or after a cybersecurity incident	CP-10, IR-4, IR-8

Data recovery capability is the ability to restore a system and / or data from a secure copy or image. Thereby allowing the restoration of a clean system. Essential information and software backup facilities should be available to help ensure recovery following a cyber incident. Retention periods and restore scenarios should be established to prioritise which critical systems need rapid restore capabilities to reduce the impact.

Additional goals for your cyber security recovery efforts may include, restoring information systems using alternate methods, performing standard operating procedures in alternate ways, recovering information systems in backup locations, and implementing contingency controls based on the business impact of the incident.

Recovery plans should be available in hard copy on-board and ashore. The purpose of the plan is to support the recovery of systems and data necessary to restore IT and OT to an operational state. To help ensure the safety of on-board personnel, the operation and navigation of the ship should be prioritised in the plan. The Recovery Plan should be understood by personnel responsible for cyber security.

The incident response team should consider carefully the implications of recovery actions (such as wiping of drives), which may result in the destruction of evidence that could provide valuable information as to the causes of an incident. Where possible, professional cyber incident response support should be obtained in order to assist in preservation of evidence whilst restoring operational capability.

Cyber security incident level (sample)

Level	Details
1	• If the information system or operating system failure time lasts more than the specified time • Prevention of the operation of information systems or operating systems • Severe damage to data cannot be recovered • Disconnecting power to information systems or operating system equipment
2	• If the information system or operating system failure time lasts less than the specified time • Some functions stop when operating an information system or operating system • Partial corruption of data required for recovery • Power supply failure of information system or operating system equipment
3	• An information system or operating system failure has occurred temporarily. • Operation of the information system or operating system is temporarily suspended • No minor damage or operation of data

System recovery priority (Sample)

Recovery priority	Influence	Urgency	RTO
1st	• Serious impact on critical business processes related to the entire organization • Serious impact on business processes that are crucial to ship operations and freight transport	High	12 hours
2nd	• Partial impact of critical business processes • Partially impacts on shipping and freight services	Medium	3days
3rd	• Minimal impact on overall organization operations • No influence of ship operation	Low	30 days

※ The time required for RTO (Recovery Time Objective) is determined by the company