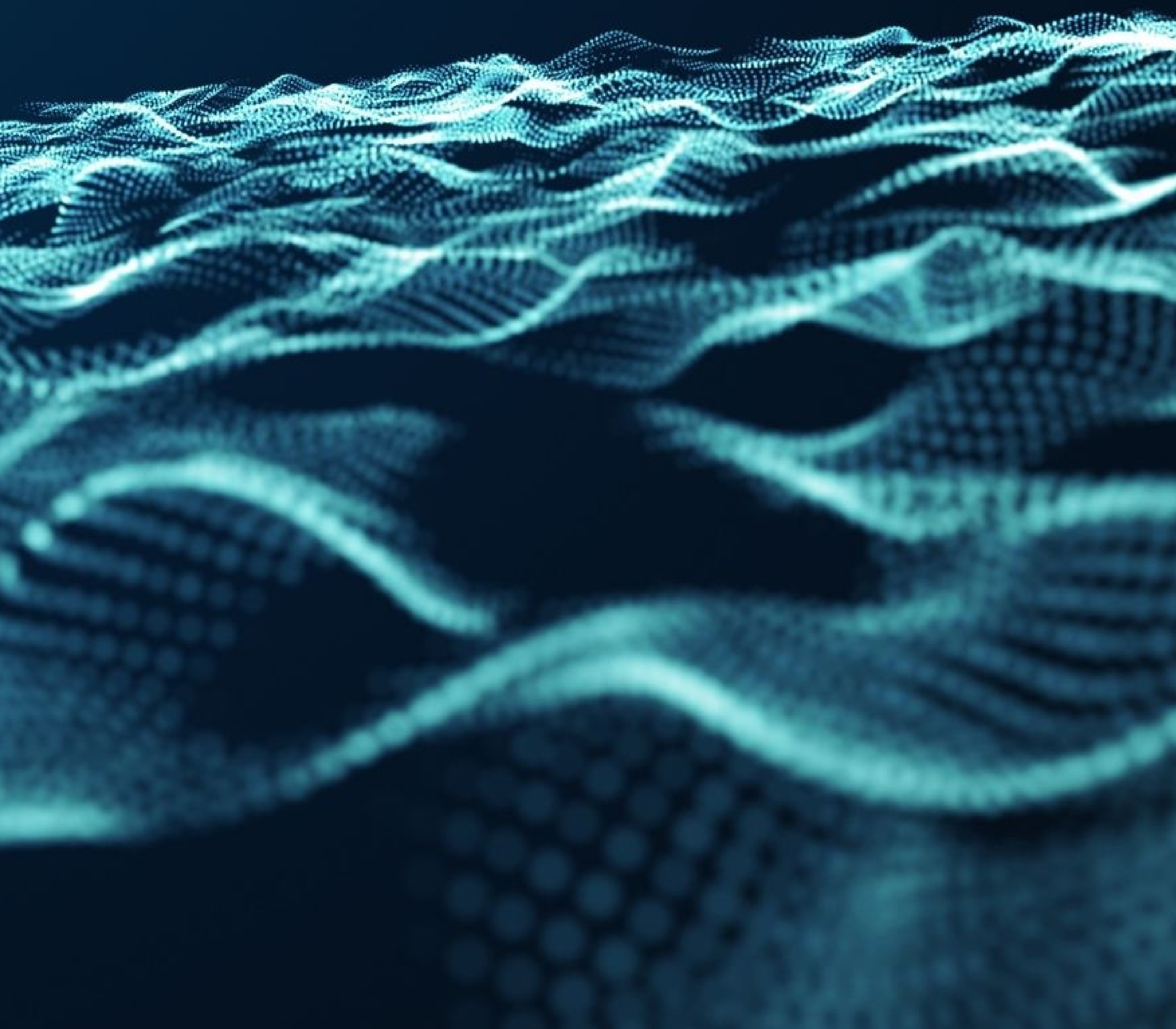
Steamship Mutual

Cyber Questionnaire



Steamship Mutual

Cyber Questionnaire

Steamship Mutual’s Cyber Insurance not only gives Members protection for losses arising out of a cyber-attack, but also gives Members quick access to cyber experts who can respond to the incident and assist the Members to resolve any issues.

Members who purchase the cover will benefit from a free Maritime Cyber Security Awareness education course, which focuses on increasing crew awareness of cyber threats. Your crew will learn the benefits of reporting all cyber incidents. As well as 10 essential steps to maritime cyber security, the course includes modules on Cyber threat, Phishing, Surfing the web, Malware & Insider threat.

The statements and representations contained in this Questionnaire shall be deemed material to the risk assumed by **the Association**, and any Policy is issued in reliance upon the truth thereof.

Company Name ____________________

Address ____________________

Name ____________________

Job title ____________________

Date ____________________

© Steamship Insurance Management Services Limited 2021

1 IDENTIFY

A Regulatory Compliance

		SHORE	ONBOARD
1.	Are cyber security management (“CSM”) procedures in place under the ISM Code?	N/A	N/A
	a) Has the CSM plan been audited?	N/A	N/A
	b) Date of last audit?	20-Feb-2	20-Feb-2
	c) Number of open major non-conformities?	N/A	N/A
2.	Are cyber roles and responsibilities defined?	N/A	N/A
3.	Is role-based cyber, data and privacy training provided to staff?	N/A	N/A

B Cyber Risk / Vulnerability / Threat Assessments

		SHORE	ONBOARD
1.	Have business and safety critical systems been identified?	N/A	N/A
2.	Is a registry of these systems maintained? *i.e. network devices, end points and data communication flows?*	N/A	N/A
3.	Are hardware / software risk assessments employed for the following?		
	a) IT systems	N/A	N/A
	b) OT systems	N/A	N/A
	c) Network systems	N/A	N/A
	d) Ship-shore communications	N/A	N/A
	e) Is assessment periodically carried out against known vulnerabilities	N/A	N/A
4.	Has business critical data been identified?	N/A	N/A
5.	Is a register of identified data maintained? *i.e. electronic records of crew, ship certificates and data subject to privacy regulation?*	N/A	N/A

© Steamship Insurance Management Services Limited 2021

6.	Have ship and shore data transfer risks been evaluated?	N/A	N/A

2 PROTECT

A Is the cyber management strategy in accordance with international standards:

1	ISO27001	N/A	N/A
2	IEC62443	N/A	N/A
3	class approval		

B User authorisation management

1	Are individual accounts used on board?	N/A	N/A
2	Do procedures require regular management of passwords?	N/A	N/A
	a) Are manufacturers default passwords changed?	N/A	N/A
3	Are tier levels employed authorising different levels of user access? *i.e. administer /privilege users*	N/A	N/A

C Cyber security familiarisation and training

1	Do *familiarisation checklists* include cyber security policies and procedures?	N/A	N/A
2	Do office staff and crew annually receive updates and training that cover:		
	a) Phishing	N/A	N/A
	b) Social engineering	N/A	N/A
	c) Ransomware	N/A	N/A
	d) Other – please list		
3	Are cyber security drills carried out?	N/A	N/A
	a) Frequency	Monthly	Monthly

© Steamship Insurance Management Services Limited 2021

	b) Date of last drill		
4	Does the company have a policy on use of personal devices?	N/A	N/A

D Physical Access

1	Is physical access to critical systems controlled?	N/A	N/A

E Portable devices / USB use policy

1	When mobile or portable devices are used in maintenance or updating of systems, are these devices scanned for malware and are they authorised for this sole purpose?	N/A	N/A
2	Are USB port blocker or end point protection devices applied on key IT /OT equipment?	N/A	N/A
3	Are procedures in place for third party USB access to vessel computers? *i.e. surveyor requesting documents to be printed*	N/A	N/A
4	What do these procedures include?		

F Hardware / Software Management

1	Are there system patching / updates in place?	N/A	N/A
2	Are firmware / hardware maintenance procedures in place and recorded?	N/A	N/A
	a) Are records and service reports maintained?	N/A	N/A
3	Software patch installation:		
	a) IT Systems – are updates carried out within 30 days?	N/A	N/A
	b) OT equipment – at the earliest opportunity as per manufacturer release?	N/A	N/A
4	Are systems actively supported by manufacturer for new vulnerabilities and threats?	N/A	N/A
5	Are critical systems periodically inspected where possible for the accuracy of the system output i.e. lines of position on an ECDIS unit?	N/A	N/A

© Steamship Insurance Management Services Limited 2021

6		Are ENC updates complete with established procedures?	N/A	N/A
	a)	Are automatic updates appropriately firewalled?	N/A	N/A
7		Does the CSM included management of change procedures?	N/A	N/A
		If yes, are the following implemented:		
	a)	Does this include purchase and installation of IT/OT equipment?	N/A	N/A
	b)	Does the company have a process of securely disposing of electronics waste?	N/A	N/A
8		Is Office 365 employed on board the applicant's vessel?	N/A	N/A
		If yes, are the following implemented:		
	a)	Microsoft 365 Advanced Threat Protection?	N/A	N/A
	b)	Multifactor authentication for all Microsoft 365 users?	N/A	N/A

G IT, OT, Network Protection

1			Connection Protocols:		
	a)		Are OT systems connection to the internet?	N/A	N/A
	b)		Is the WI-FI access regulated and password controlled?	N/A	N/A
	c)		Does the vessel have integrated systems? *i.e. Integrated bridge or vessel monitoring system*	N/A	N/A
	d)		Is Remote Desktop Protocol enabled?	N/A	N/A
		i	VPN access only?	N/A	N/A
		ii	Multi-factor authentication for access?	N/A	N/A
		iii	Network level authentication enabled?	N/A	N/A
		iv	RDP honeypots(s)?	N/A	N/A

© Steamship Insurance Management Services Limited 2021

v	Identify any other protocols		
vi	Is the vessel adequately supported from the onshore cyber system team?	N/A	N/A
vii	Are business networks isolated from crew networks?	N/A	N/A
viii	Is personal crew access to business computers restricted?	N/A	N/A
2	Protection Methods		
a)	Are systems installed with anti-virus?	N/A	N/A
b)	Is multi-factor authentication required for the following access:	N/A	N/A
i	Critical Information?	N/A	N/A
ii	Remote Access?	N/A	N/A
iii	Administration Level Access?	N/A	N/A
iv	Personal Devices?	N/A	N/A
v	Non-Critical information?	N/A	N/A
c)	Are your network systems segregated?	N/A	N/A
d)	OT system hardening as provided by manufacturer adopted such as in case of main engine control system?	N/A	N/A
e)	Are protocols such as IP network, encryption, VPN connections etc adopted?	N/A	N/A
f)	Has an endpoint detection and response package been deployed at corporate and vessel level?	N/A	N/A

H Back-up arrangements

1	Are periodical back-up arrangements in place for critical systems data and business data (identified in Section 1 B4 and C2)	N/A	N/A
a)	If so, what frequency:	Never	Never

© Steamship Insurance Management Services Limited 2021

	b) Is the back-up data encrypted?	N/A	N/A
	c) Is the back-up data stored on a server on board?	N/A	N/A
	d) Is this server connected to the internet?	N/A	N/A
	e) Are physical back-up tapes used?	N/A	N/A
	f) Where are the shore-side back-ups stored?		
	i Cloud	N/A	N/A
	ii On premises	N/A	N/A
	iii Offline storage	N/A	N/A
	iv Offsite storage	N/A	N/A
	v Secondary data centre	N/A	N/A
	vi ID any other		
2	What cyber security measures are applied to back-ups To select hold shift and click your response	None Multifactor Authenticatio Encryption Segmentation Virus Malware Scanning	None Multifactor Authenticatio Encryption Segmentation Virus Malware Scanning
3	Are unique backup credentials stored separately from other credentials?	N/A	N/A
4	Are physical and systematic barriers in place to mitigate loss of live and back-up data resulting from a cyber incident for the following systems?		
	a) IT systems	N/A	N/A
	b) OT systems	N/A	N/A

© Steamship Insurance Management Services Limited 2021

5	How frequently are back-ups made to offsite storage?		
	a) Weekly	□	□
	b) Monthly	□	□
	c) Quarterly	□	□
6	How frequently is a full recovery from a back-up tested		
	a) Weekly	□	□
	b) Quarterly	□	□
	c) Annually	□	□
	d) Not tested	□	□

I Email, data and communications policy

1	Does email protocol employ solutions such as?	N/A	N/A
	a) Sender Policy Framework (SPF)?	N/A	N/A
	b) DKIM?	N/A	N/A
	c) DMARC?	N/A	N/A
	d) Other		
2	Are email accounts and recovery encrypted?	N/A	N/A
3	Does the vessel employ any cloud-based IT infrastructure?	N/A	N/A
4	Are policies and procedures in place to deal with the third-party digital data connectivity and data exchange? *i.e. supply chain cargo information to charter*	N/A	N/A

© Steamship Insurance Management Services Limited 2021

3 DETECT

A Intrusion detection

1	Is intrusion detection / protection software employed on all corporate and vessel level IT system?	N/A	N/A
2	Does the vessel use a checklist or procedure for a cyber-attack such as BIMCO cyber handbook and checklist?	N/A	N/A
3	Are processes in place to detect Global Navigation Satellite System (GNSS) spoofing/jamming and take appropriate responsive action (navigating without digital aids etc)?	N/A	N/A
4	Are there procedures in place for reporting cyber related incidents and attacks to the office, including human error?	N/A	N/A

B Log Monitoring

1	Are procedures in place to monitor administrator access for suspicious or unusual activity i.e. Review of activity for larger than normal amounts of data been transferred or deleted?	N/A	N/A
	a) Are these procedures recorded for audit purposes?	N/A	N/A

4 RESPOND

A Incident response / contingency plan

1	Is a cyber-attack response/contingency plan available?	N/A	N/A
	If so, does it contain the following assessments:		
	a) Immediate actions to be taken and assessment of seaworthiness?	N/A	N/A
	b) Isolation of affected systems or default to pre-cyber event condition?	N/A	N/A
	c) Shifting to alternative methods	N/A	N/A

© Steamship Insurance Management Services Limited 2021

	i Is there stand-alone equipment i.e. radar, ECDIS unit to deal with any integrated cyber-attack?	N/A	N/A
	ii Satcom – Is it protected by a firewall	N/A	N/A
	iii Is the system updated to the latest version?	N/A	N/A
	d) Responsible person to notify?	N/A	N/A
2	Is there a ransomware specific incident response plan in line with international guidance?	N/A	N/A
3	Are there response tools/software to deal with malware?	N/A	N/A
4	Are there sufficient cyber committee and emergency response support available to vessels for operational and emergency issues?	N/A	N/A

5 RESTORE

1	Are there procedures in place to recover data from the following systems and if so, please indicate the recovery point objective:		
	a) IT systems	N/A	N/A
	i Time period		
	b) OT Systems	N/A	N/A
	ii Time period		
2	Are policies and procedures in place for the recovery of onboard safety and business critical systems within a defined period (recovery time objective) to the pre-incident standard of operation?	N/A	N/A
	a) Time period		
3	Are procedures in place for recovered systems to be tested, verified and where required reapproval from Class?	N/A	N/A

© Steamship Insurance Management Services Limited 2021

Thank you for completing our CyberQuestionnaire. Please print the completed questionnaire to pdf to lock your responses, and forward the completed document to your usual Steamship Mutual contact.

Steamship Mutual

STEAMSHIP MUTUAL UNDERWRITING ASSOCIATION LIMITED
Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and Prudential Regulation Authority
(Registered in England and Wales – Registration number 105461. PRA and FCA registration number 202548)

MANAGERS: STEAMSHIP P&I MANAGEMENT LLP
SPIM is an appointed representative of Steamship Insurance Management Services Limited
which is authorised and regulated by the Financial Conduct Authority
(Registered in England and Wales – Registration Number OC376859. FCA registration number 597046)
AQUATICAL HOUSE 39 BELL LANE LONDON E1 7LU
Tel: +44 20 7247 5490 Website: www.steamshipmutual.com

© Steamship Insurance Management Services Limited 2021