TECHNICAL CIRCULAR No. 546 of 04th April 2019

To:	All Surveyors/Auditors
Applicable to flag:	All Flags
	How to prepare for Cyber Security
Reference:	Cyber Security

How to prepare for Cyber Security

Shipping companies are in many areas of risk management, such as the environmental side, security and other key areas, but we started to see about 5 years ago that cyber was going to be something important and understanding how the vessel owners we serve approach new problems like this.
Cyber Security is in regulations, it is in the ISM Code, not by name necessarily, but by the fact that you are already required right now to establish safeguards when you identify a risk.
BIMCO, CLIA, ICS, Intercargo, Intertanko, etc. said this risk is real. BIMCO has come up with two things in particular: They have recognized that most shipping companies are going to need external assistance and that assistance is going to be like in other areas:

- Before a cyber incident
- During a cyber incident and
- After a cyber incident

Another thing that BIMCO guidelines says is 'Establish a team'. The team needs to be established to take the appropriate actions. It must be capable, in other words, not the guys you know around the corner, not the guy you trust and like very well, who had a graduate degree in IT. He may be good, but this is a capability-driven requirement. You've got to have capabilities. That team must be identified in your plan.
So if you are trading to the US and you experience an incident on your vessel or an incident that will affect you vessel, you need right now a reasonable chance of risk, a threatened incident; there is a reporting requirement now.

Before an attack occurs:

- ***Assess***: Perform a cybersecurity capability assessment of your entire organization: How cyber secure are you, how capable are you, how mature are you?

Customer Service Center
5201 Blue Lagoon Drive, 9TH. Floor,
Miami, Fl., 33126
Tel: 1 (305) 716 4116,
Fax: 1 (305) 716 4117,
E-Mail:
joel@conarinagroup.com

Technical Head Office
7111 Dekadine Ct.
Spring, Tx., 77379
Tel: 1 (832) 451 0185,
1 (713) 204 6380
E-Mail: vbozenovici@vcmaritime.com

- ***Plan***: Establish a cyber **incident response (IR) plan.** This plan must be a real plan, based on your real vessels, on your real enterprise, your business, based on your real operating systems and your IT systems.
- **Train:** Incorporate cyber risks into tabletop exercises. We had an awareness training. Is that all you need? No. Awareness training is great, but it is a starting point.
- **Integrate Plans: Data Loss Prevention** (DLP), **Disaster Recovery** (DR) and **Business Continuity Plans** (BCP). Does the plan you have on cyber really work with the other plans that you are already using for your business?

REFERENCES:

- Cyber Security, by Cynthia Hudson

- ATTACHMENTS: No

Kindest Regards,

Val Bozenovici
Naval Architect – Conarina Technical Director

Customer Service Center
5201 Blue Lagoon Drive, 9TH. Floor,
Miami, Fl., 33126
Tel: 1 (305) 716 4116,
Fax: 1 (305) 716 4117,
E-Mail:
joel@conarinagroup.com

Technical Head Office
7111 Dekadine Ct.
Spring, Tx., 77379
Tel: 1 (832) 451 0185,
1 (713) 204 6380
E-Mail: *vbozenovici@vcmaritime.com*