TECHNICAL CIRCULAR No. 438 of 04th October 2017

To:	All Surveyors/Auditors
Applicable to flag:	All Flags
	Managing Human Cyber Risks in the Maritime Industry
Reference:	Cyber Security

Managing Human Cyber Risks in the Maritime Industry

While automation is an attractive proposition for ship-owners, it also brings complexity because its introduction requires more than the simple replacement of the functions of older systems.
The key to effective systems-risk assessment and management – digital or otherwise – lies in building human understanding of how those systems work. It is a challenge that largely can be met by combining current methods of both industrial and human engineering.
As systems gain complexity, efforts to reduce the potential for human error need to be redoubled.
Workforce risks can also be mitigated by strengthening policies that limit access to specific systems, segregating networks, filtering emails and installing browser blocks.
From an engineering perspective, the integration of systems makes sense; modern systems are built to encourage the consolidation of functions. Their builders incorporate network links where it makes sense for systems to use connectivity and provide interoperability. It is part of automation's attraction.
However, inter-system connections can introduce unanticipated communications paths, which complicates matters on many levels, from systems security to employee training.
Crews and operators are trained according to the methods and functions for which systems are originally designed and built. The characteristics and performances of individual systems are largely documented by their designers; understanding the behavior of systems that are connected, integrated and/or interdependent is more complex. The potential for disruption often multiplies beyond the sum of the parts.

Developing an organizational cyber culture is similar to developing a safety culture in that a well-defined structure will help to engineer risks – human or industrial -- down to acceptable levels.
From a human engineering perspective, the basics of a healthy organizational cyber culture will include (but not be limited to):
- Company-specific programs that build an understanding of cyber risks
- Strategies for employee engagement (to build knowledge and situational awareness, and to

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: cbozenovici@vcmaritime.com

avoid complacency)
- The creation of a just culture in which workers are seen to be treated fairly (this is different than a no-blame culture in that it includes worker accountability)
- A commitment to employee empowerment (to help them fulfill their responsibilities)
- The promotion of personal integrity (so employees do the right thing, even when no one is looking)
- A visible commitment to cyber resilience from the corporate leadership
- Effective communication practices (including positive and negative feedback)

Decades of dedication to building maritime safety awareness has provided us with the human and industrial engineering practices and methodologies that are now required to build cyber resilience across an increasingly connected modern systems architecture.

REFERENCES:

- ABS Courtesy

ATTACHMENTS: No.

Kindest Regards,
Cosmin Bozenovici
Naval Architect – Conarina Technical Head Office

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: cbozenovici@vcmaritime.com