

CyberSafety® Program

PANTELIS SKINITIS | JUNE 2018

Safety Moment



Industry Drivers – Maritime Cyber Survey

34% (of 284 respondents) experienced a cyber attack within the last 12 months

- Majority Ransomware or Phishing

30% of companies did not have an information security manager or department

Many employees lacked cyber awareness training

66% had a cyber security policy

47% believed their organization's biggest cyber vulnerability was its staff



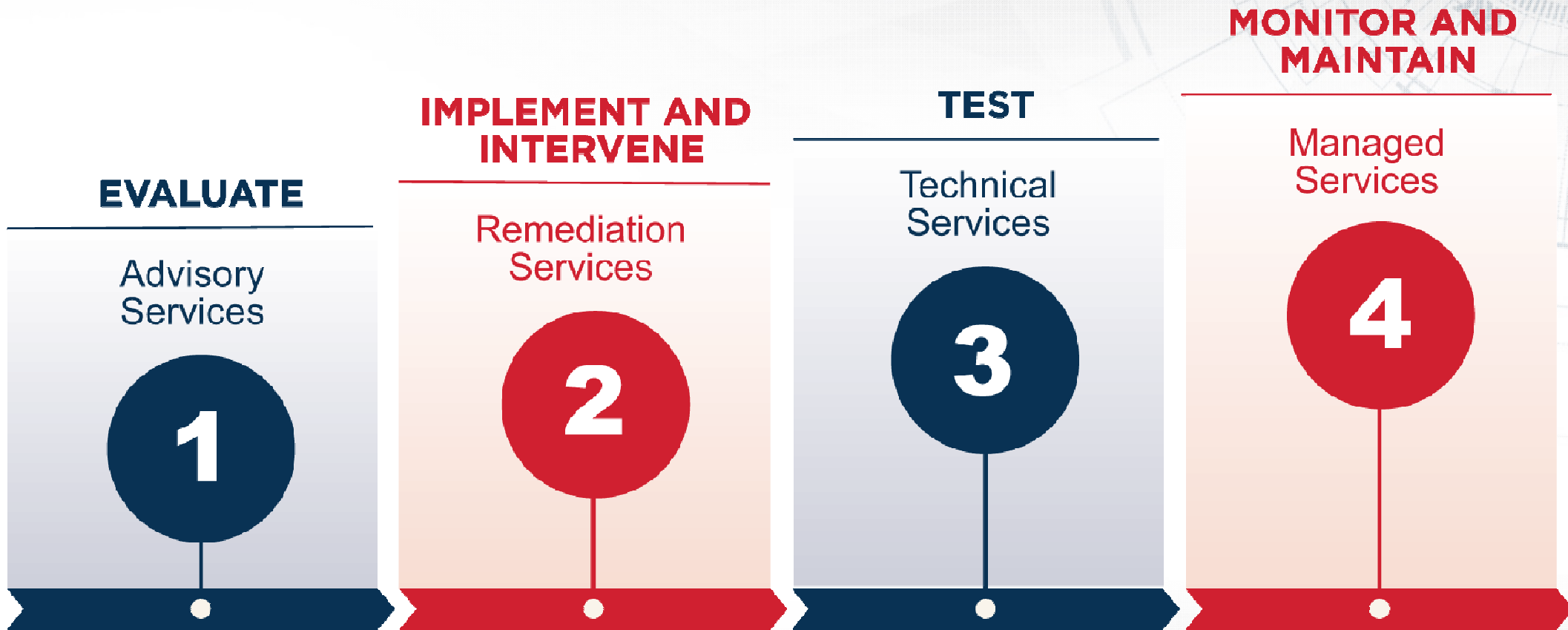
Here are Real Consequences and Differentiators

Regulatory / Industry Best Practices	Real Consequences		Differentiators
<p>USCG</p> <ul style="list-style-type: none"> - Policy Letter - NVIC 05-17 	<ul style="list-style-type: none"> • Operational 	<p>Disruption</p>	<ul style="list-style-type: none"> • Prioritizing Cyber Solutions
<p>IACS Steering Committee BIMCO/Intertanko/OCIMF Guidelines IMO 2021 Implementation UK Code of Practice</p>	<ul style="list-style-type: none"> • Damage to 	<p>Corporate Reputation</p>	<ul style="list-style-type: none"> • Evidence of Competency
<p>TMSA3 Rightship</p>	<ul style="list-style-type: none"> • Insurability 	<p>Questions</p>	<ul style="list-style-type: none"> • Satisfaction of Bid Requirements

BS Response to Industry and Regulatory Drivers



OT Cyber Maturity Journey



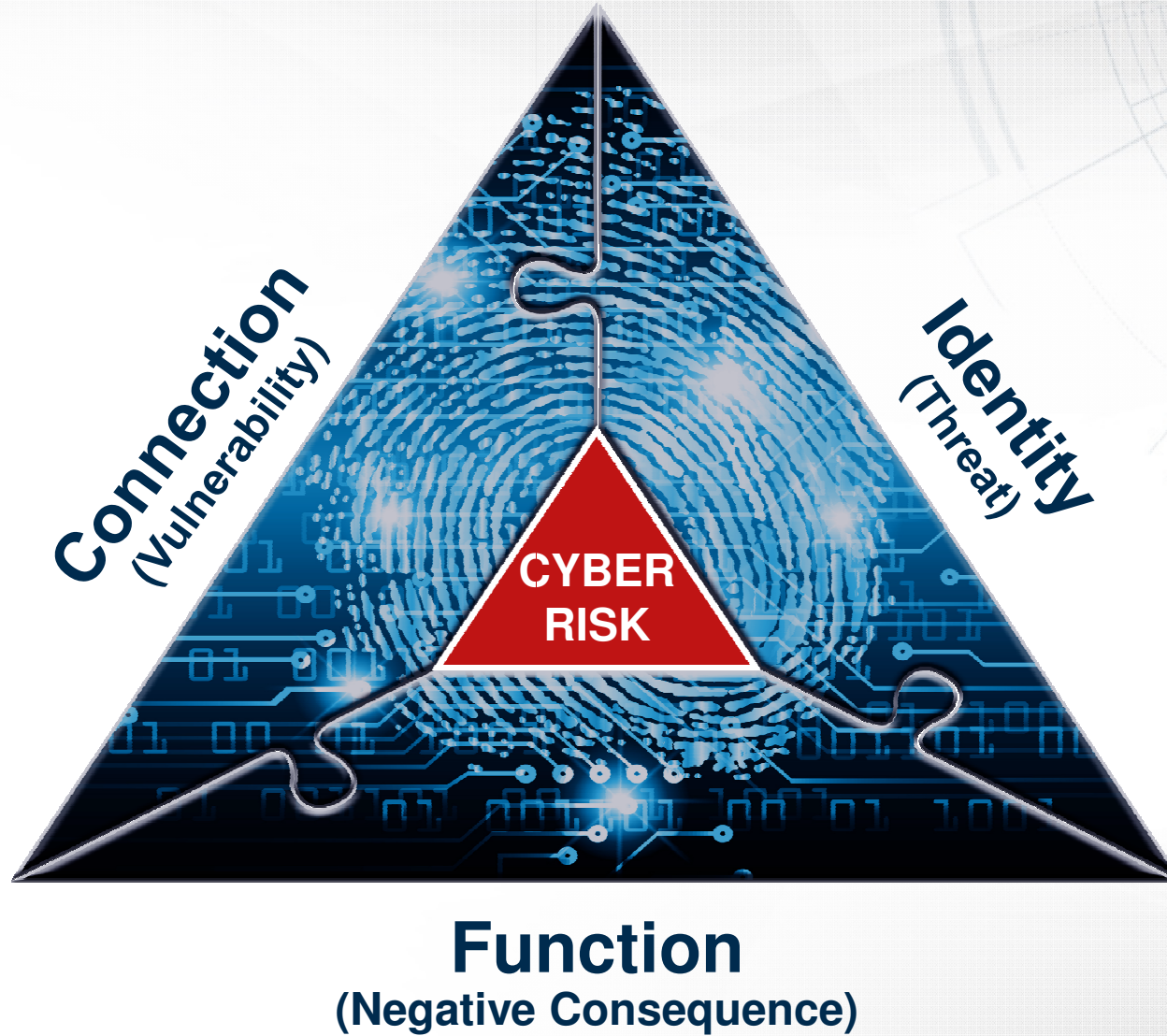
Calculable OT Cyber Risk

CI Model

Maritime specific

Measurable

Scalable



How It Works

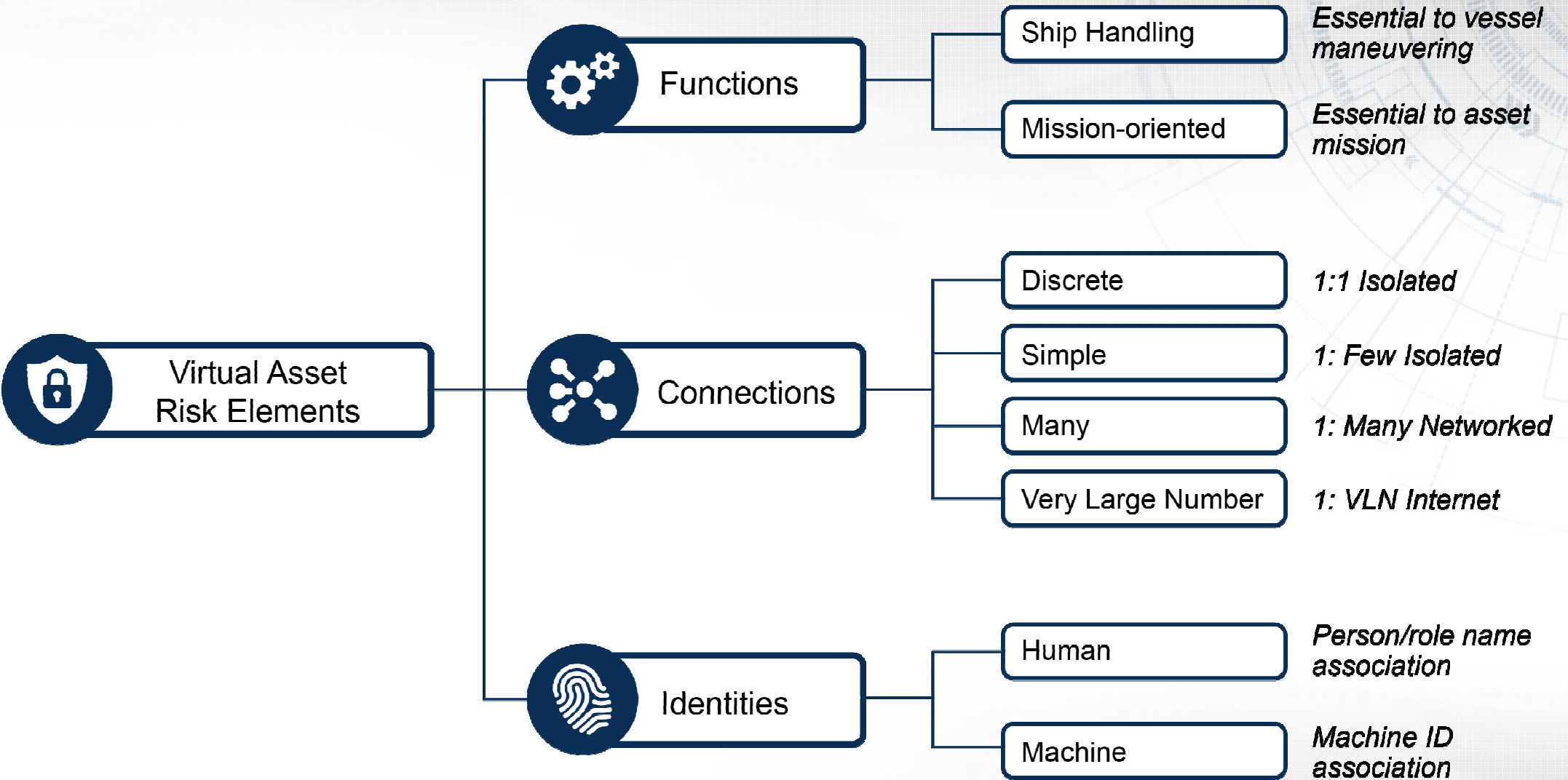


**ONSHORE DOCUMENTATION
REVIEW**



ON-ASSET SURVEY

Virtual Vessel Profile



$$\text{Risk Index} = \text{Functions} \times \text{Connections} \times \text{Identities}$$

Cyber – Calculable Risk Index

Example 1: Segmented Architecture

Set	Functions				F	Connections			Identities				Risk (CRI)			
	Function Number F _n	Member of a Set? F _s	Function Set Cardinality F _c	Connection Category F _r		Total Connections C _t	Invulnerable Connections C _i	Vulnerable Connections C _v	C	Trusted Humans I _{th}	Untrusted Humans I _{uh}	Trusted Devices I _{td}	Untrusted Devices I _{ud}	I	Risk (CRI) by function by function set	
A	1	Yes	5	VLN	25	4	2	2	1.0	25	25	25	0	1.1	28	
	2	Yes	5	VLN	25	4	2	2	4.0	25	25	25	0	1.0	100	
	3	Yes	5	VLN	25	3	2	1	0.5	25	25	25	0	1.0	13	
	4	Yes	5	VLN	25	3	2	2	1	0.5	25	25	25	0	1.0	100
	5	Yes	5	VLN	25	3	2	2	1	0.5	25	25	25	0	1.0	13
B	6	Yes	4	Complex	12	3	2	1	0.5	13	25	25	0	1.0	13	
	7	Yes	4	Complex	12	3	2	1	0.5	13	25	25	0	1.0	13	
	8	Yes	4	Complex	12	2	2	2	0.0	13	25	25	0	1.0	13	
	9	Yes	4	Complex	12	2	2	2	0.0	13	25	25	0	1.0	13	
C	10	Yes	4	Complex	12	2	2	1	0.5	13	25	25	0	1.0	13	
	11	No	1	Discrete	1	2	1	0	0.0	13	25	25	0	1.0	13	
	12	No	1	Discrete	1	2	1	0	0.0	13	25	25	0	1.0	13	
D	13	No	1	Discrete	1	6	2	1	1.0	13	3	13	3	0.5	0	
	14	No	1	Discrete	1	7	0	0	0.0	13	3	13	3	0.5	0	
E	15	No	1	Discrete	1	5	6	0	6.0	13	3	13	3	0.5	0	
	16	No	1	Discrete	1	4	1	1	0.2	8	2	13	3	0.5	6	
F	17	No	1	Discrete	1	5	5	0	1	6	3	13	3	0.5	0	
	18	No	1	Discrete	1	4	1	1	0.2	7	1	8	3	0.5	6	
Total					49	4	4	1	0.2	4	1	7	1	0.3	0.042	

Example 2: Integration of Safety-critical OT Systems

Set	Functions				F	Connections			Identities				Risk (CRI)			
	Function Number F _n	Member of a Set? F _s	Function Set Cardinality F _c	Connection Category F _r		Total Connections C _t	Invulnerable Connections C _i	Vulnerable Connections C _v	C	Trusted Humans I _{th}	Untrusted Humans I _{uh}	Trusted Devices I _{td}	Untrusted Devices I _{ud}	I	Risk (CRI) by function by function set	
A	1	Yes	5	VLN	25	4	2	2	1.0	25	25	25	0	1.1	28	
	2	Yes	5	VLN	25	4	2	2	4.0	25	25	25	0	1.0	100	
	3	Yes	5	VLN	25	3	2	1	0.5	25	25	25	0	1.0	13	
	4	Yes	5	VLN	25	3	2	2	1	0.5	25	25	25	0	1.0	100
	5	Yes	5	VLN	25	3	2	2	1	0.5	25	25	25	0	1.0	13
B	6	Yes	4	Complex	12	3	2	1	0.5	13	25	25	0	1.0	13	
	7	Yes	4	Complex	12	3	2	1	0.5	13	25	25	0	1.0	13	
	8	Yes	4	Complex	12	2	2	2	0.0	13	25	25	0	1.0	13	
	9	Yes	4	Complex	12	2	2	2	0.0	13	25	25	0	1.0	13	
C	10	Yes	4	Complex	12	2	2	1	0.5	13	25	25	0	1.0	13	
	11	Yes	4	Simple	8	2	1	0	0.0	13	3	13	3	0.3	13	
	12	Yes	4	Simple	8	2	1	0	0.0	13	3	13	3	0.3	13	
D	13	Yes	4	Simple	8	6	2	0	6.0	13	2	13	3	0.5	0	
	14	Yes	4	Simple	8	6	2	0	6.0	13	2	13	3	0.5	0	
E	15	No	1	Discrete	1	5	5	1	0.2	6	3	13	3	0.5	6	
	16	No	1	Discrete	1	4	1	1	0.2	7	1	8	3	0.5	6	
F	17	No	1	Discrete	1	5	4	1	0.3	7	1	7	1	0.3	22	
	18	No	1	Discrete	1	4	1	1	0.3	7	1	7	1	0.3	0	
Total					54	34	20	0.3	0.3	4	1	4	1	0.3	0	

Example 3: Inadvertent Integration of IT & OT Systems

Set	Functions				F	Connections			Identities				Risk (CRI)			
	Function Number F _n	Member of a Set? F _s	Function Set Cardinality F _c	Connection Category F _r		Total Connections C _t	Invulnerable Connections C _i	Vulnerable Connections C _v	C	Trusted Humans I _{th}	Untrusted Humans I _{uh}	Trusted Devices I _{td}	Untrusted Devices I _{ud}	I	Risk (CRI) by function by function set	
A	1	Yes	5	VLN	25	4	2	2	1.0	25	25	25	0	1.1	28	
	2	Yes	5	VLN	25	4	2	2	4.0	25	25	25	0	1.0	100	
	3	Yes	5	VLN	25	3	2	1	0.5	25	25	25	0	1.0	13	
	4	Yes	5	VLN	25	3	2	2	1	0.5	25	25	25	0	1.0	100
	5	Yes	5	VLN	25	3	2	2	1	0.5	25	25	25	0	1.0	13
B	6	Yes	4	Complex	12	3	2	1	0.5	13	25	25	0	1.0	13	
	7	Yes	4	Complex	12	3	2	1	0.5	13	25	25	0	1.0	13	
	8	Yes	4	Complex	12	2	2	2	0.0	13	25	25	0	1.0	13	
	9	Yes	4	Complex	12	2	2	2	0.0	13	25	25	0	1.0	13	
C	10	Yes	4	Complex	12	2	2	1	0.5	13	25	25	0	1.0	13	
	11	Yes	4	Simple	8	2	1	0	0.0	13	3	13	3	0.3	13	
	12	Yes	4	Simple	8	2	1	0	0.0	13	3	13	3	0.3	13	
D	13	Yes	4	Simple	8	6	2	0	6.0	13	2	13	3	0.5	0	
	14	Yes	4	Simple	8	6	2	0	6.0	13	2	13	3	0.5	0	
E	15	No	1	Discrete	1	5	4	1	0.2	7	1	7	1	0.3	22	
	16	No	1	Discrete	1	4	1	1	0.3	7	1	7	1	0.3	0	
F	17	No	1	Discrete	1	5	4	1	0.2	8	2	13	3	0.5	6	
	18	No	1	Discrete	1	4	1	1	0.2	7	1	8	3	0.5	6	
Total					57	34	23	0.3	0.3	4	1	4	1	0.3	0	

Leading OT Cyber Safety in Maritime

CyberSafety Assessment

- We assess where your current cyber state
- We provide a GAP analysis with actionable insight
- We recommend an implementation plan to fill gaps

Program Standup

- We can implement the entire program for you



Trusted Expertise

ABS awarded research contract by the Maritime Security Center (MSC) to lead industry partnership to determine direction of cyber security in maritime industry

“This research project will support the missions of the DHS Center of Excellence and the U.S. Coast Guard to address these concerns and vulnerabilities and will identify policies and risk management strategies to bolster the cyber security posture of the MTS enterprise.”

MAJOR INDUSTRY RECOGNIZED CERTIFICATIONS:

PE (CONTROL SYSTEMS), CISSP, GICSP, CISA, CCNA, CCNP, SOFTWARE QUALITY CONTROL, PMP, ICS-CERT

200+ YEARS OF CUMULATIVE
CYBER EXPERIENCE
IN MARINE APPLICATION

CYBER SECURITY ASSESSMENT OF
30+ MARINE/OFFSHORE
ASSET TYPES

FOR VARIOUS OWNERS

- NAVIGATION
- CONTROL SYSTEMS
- SURVEILLANCE SYSTEMS



Cyber Notation



7/Shutterstock

Our Commitment to You



SAFETY FIRST



OPERATIONAL EXCELLENCE



AGILITY



RELIABILITY

We've made solving industry challenges the focal point of our approach on the ABS Advanced Solutions team.

Soar Above the Challenge

www.eagle.org

