



Cyber Security Best Practices for Tankers & TMSA 3 / VIQ 7 Compliance

Digital Ship



MARITIME CYBER
RESILIENCE FORUM

ATHENS, 7 MAY 2019

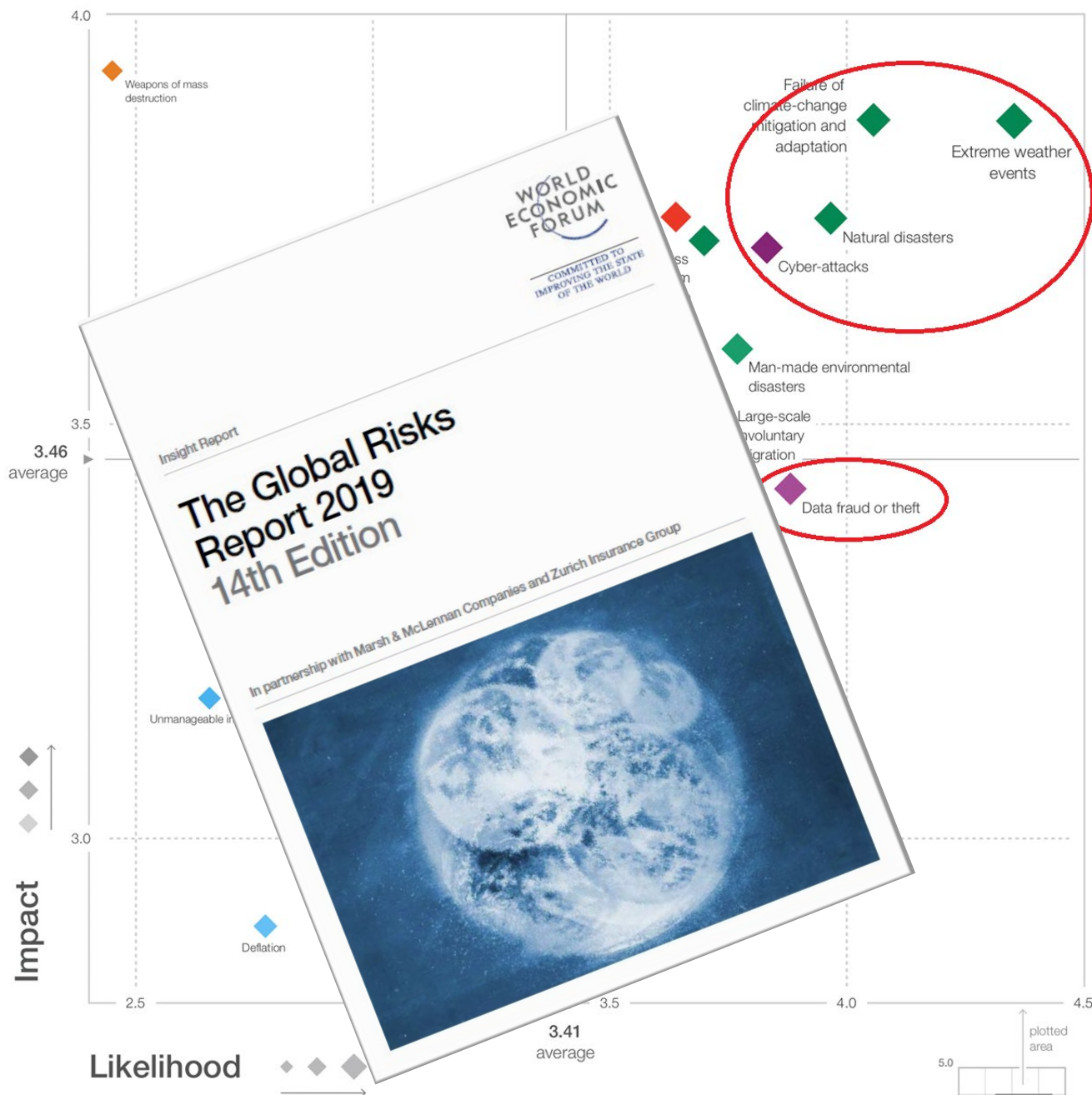
Dr. Matthew Maheras
IT Manager
Metrostar Management Corp.

Global Risks Landscape



Top 10 Likelihood

- 1 Ext
- 2 Fai
- 3 Na
- 4 Da
- 5 Cyl
- 6 Ma
- 7 Lar
- 8 Bic
- 9 Wa
- 10 Ass

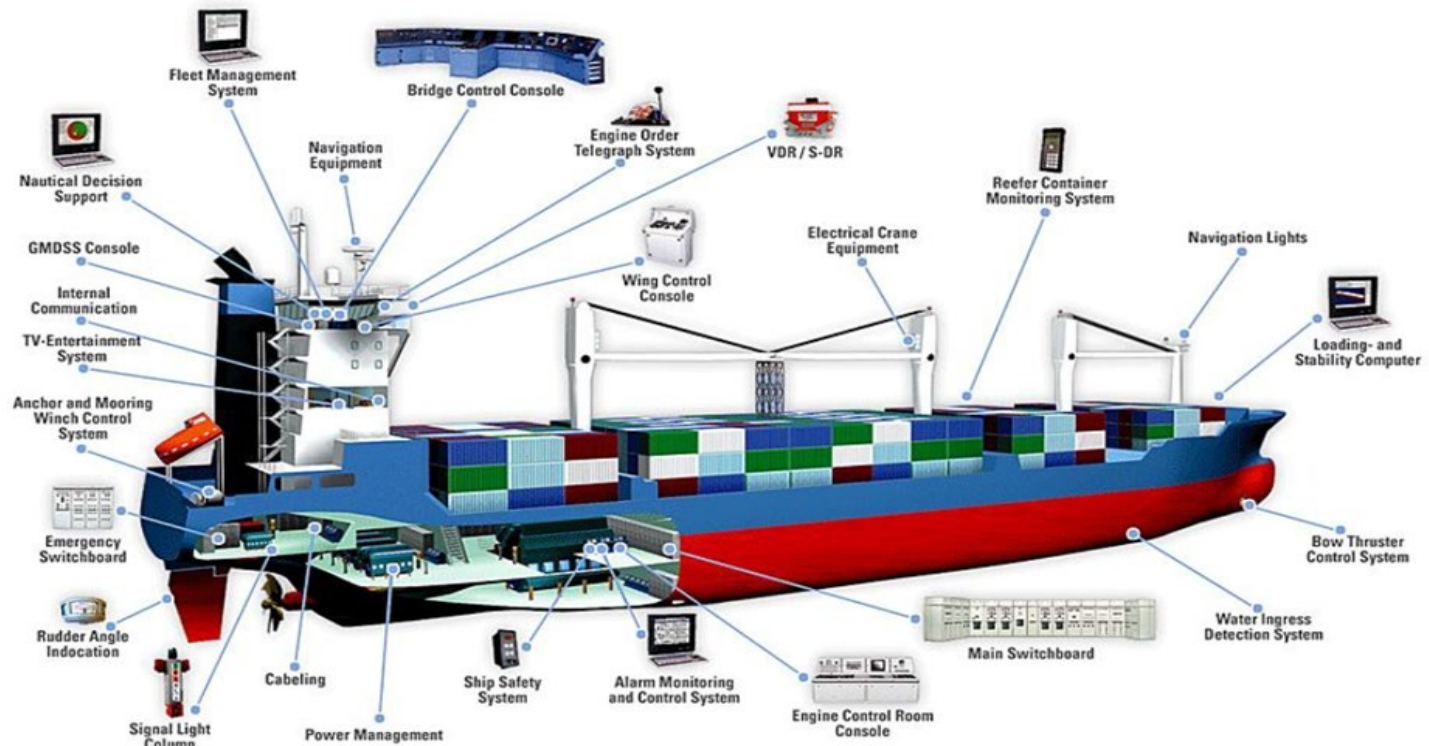


d adaptation

se

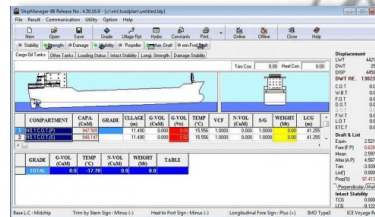
down

IoT and OT Onboard Ships



Which shipborne systems are most vulnerable?

- | | | |
|----------------|-----------------------------|--|
| A ECDIS | D Positioning system | G Cargo control systems |
| B VDR | E BNWAS | H Engine control and monitoring systems |
| C IBS | F GMDSS | I Other |



Source: IHS Maritime & Trade
Written by: Meritas, 05/10/2014

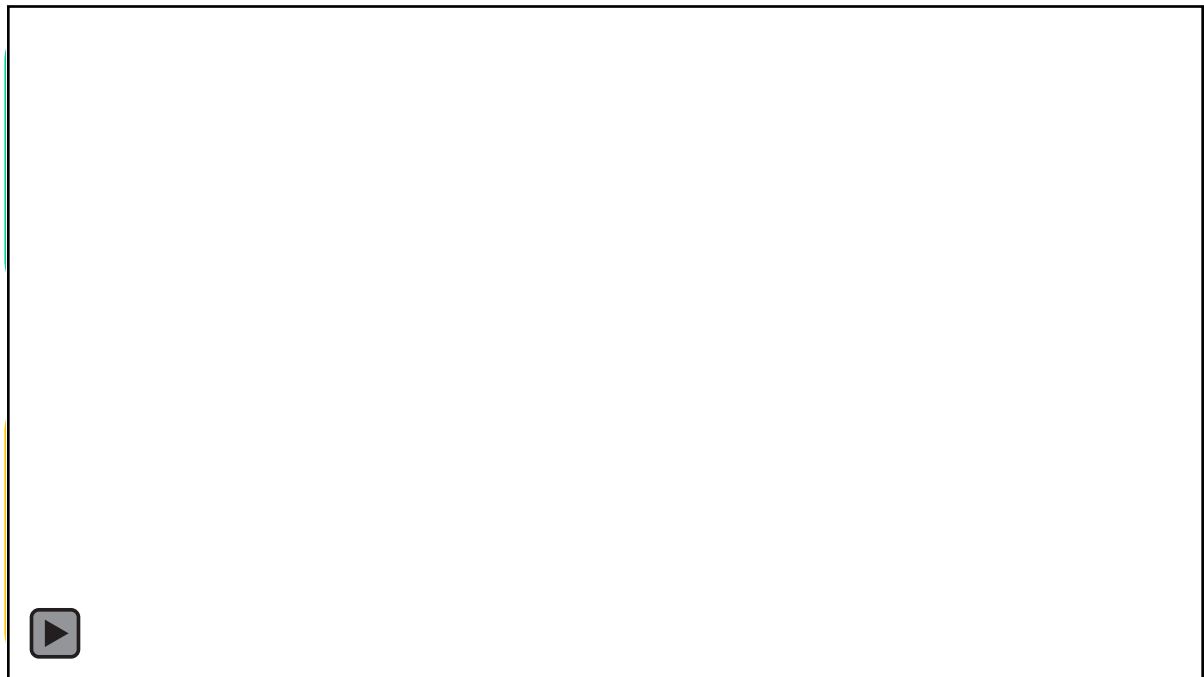
© 2016 IHS: 1017218



Common IT & OT Vulnerabilities

Mostly covered by existing
IT Cyber Security Policy

OT - specific vulnerabilities
not previously considered





Traffic Live Map Vessels Ports Companies Community Solutions Vessel

it's a Crude Oil Tanker en route! :-)

Create notifications for this Vessel Fleet control

Gross Tonnage: 31
Deadweight: 31
Length Overall x Breadth Extreme: 333m x 60m
Year Built: 2012
Status: Active

Companies at Destination

ETA : 2018-09-27 03:30 LT (UTC +5.5)

Route Forecast

Distance: 20.6m

Speed (Max /): 11.3 / 7.8 knots

Reported ETA Received: 2018-09-14 20:09 LT (UTC +3)

Intellian Aptus Web v1.20

bin/getagent.cgi?type=1

Intellian® Signal Level 144 Setup Initial Search Track TX Enable Restart Setup Save Sat. Ant. Info Account Logout

Dashboard

Current Antenna Position / Target Antenna Position

Relative Azimuth(°)	59.28
Absolute Azimuth(°)	158.28 / 158.97
Elevation(°)	59.30 / 59.31
LNB Pol Angle(°)	-19.10 / -23.91

GPS

Longitude(°)	59.381901	E
Latitude(°)	24.89566	N

Heading Device

Current Device: NMEA 4800

Heading(°): 90

BOW Offset

Current Bow Offset(°): 90

DVB Information

Frequency(MHz)	115
Symbol(kSps)	20000
NID	0x 0001
Verify Type	AGC Only

NBD Information

IF Frequency(kHz)	1255738
Bandwidth(kHz)	0
Base Local	10250 Mhz

Local Frequency Setting(MHz)

13V + 0kHz	9750
------------	------

Azimuth Animation

TX Enable

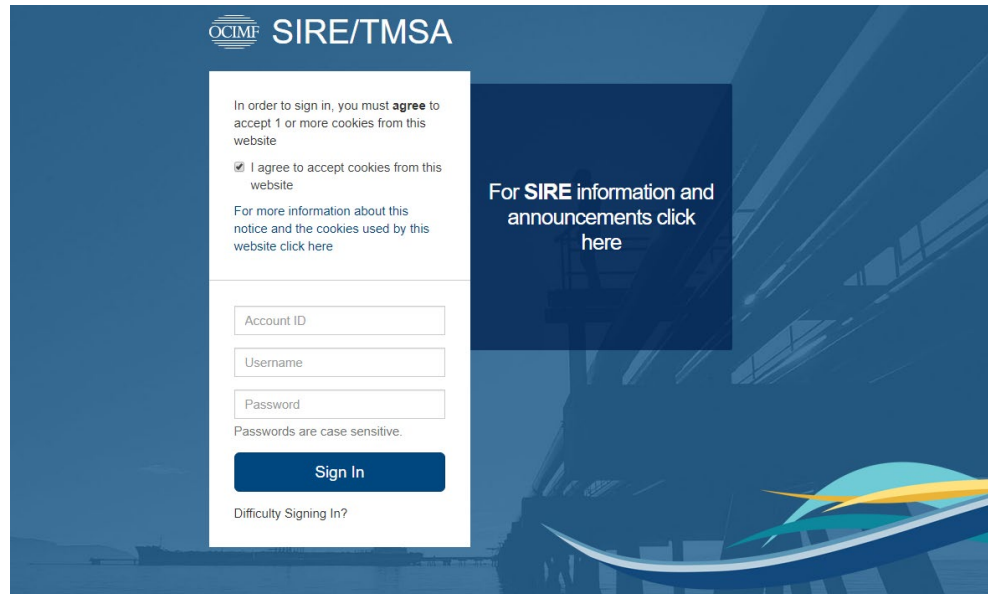
Enable Mode

Blockage

we've gained full access to Network Settings, Users Firmware, Reset, Shutdown etc.!!

11:40 7:56 μμ 16/9/2018

TMSA 3 - SIRE Integration



The screenshot shows the OCIMF SIRE/TMSA login interface. At the top left is the OCIMF logo. The main heading is 'SIRE/TMSA'. A white box contains a cookie consent message: 'In order to sign in, you must agree to accept 1 or more cookies from this website', followed by a checked checkbox 'I agree to accept cookies from this website' and a link 'For more information about this notice and the cookies used by this website click here'. Below this are input fields for 'Account ID', 'Username', and 'Password', with a note 'Passwords are case sensitive.' and a 'Sign In' button. At the bottom of the white box is a link 'Difficulty Signing In?'. To the right of the white box is a dark blue box with the text 'For SIRE information and announcements click here'. The background is a blue gradient with a stylized ship and a yellow and blue swoosh at the bottom right.

The TMSA programme and report is now fully integrated within OCIMF's Ship Inspection Report Programme (SIRE)

Provides a single area to maintain all data related to a vessel's technical operator, including; Ship Inspections, Vessel Particulars Questionnaire (VPQ), Crew Reports and Incidents



Cyber Security in SIRE / VIQ 7



OCIMF Ship Inspection Report Programme

Vessel Inspection Questionnaire Tankers, Combination Carriers, Shu Chemical Tankers and Gas Tanker Edition (VIQ 7)

Oil Companies International Marine Forum

- 7.11 Does the Master/SSO have a clear understanding of the procedures for voluntary security reporting?
- Note: Check evidence of participation in voluntary security reporting such as reporting to UKMTO when passing through the Indian Ocean.
- 7.12 Is an adequate deck watch being maintained to prevent unauthorised access in port?
- Note: There should be a continuous gangway watch and a routine for regular rounds of the deck to monitor potential access points (e.g. hose pipes; mooring ropes; etc.).
- Remote monitoring of different areas on ships is increasingly being used. Where technology such as CCTV is employed to monitor potential access points to the ship this should be noted in comments.
- 7.13 Has the company provided a list of security charts, publications and guidelines to the ship?
- Such security charts, publications and guidelines may include:
- Relevant UKHO security charts
 - Industry best management practice guidance
 - Any other company specific guidance

Cyber Security

- 7.14 Are Cyber Security Policy and Procedures part of the Safety Management System and is there a Cyber Response Plan onboard?
- Note: Do the procedures include a risk assessment of issues such as:
- Threats such as from malware; phishing attacks etc.
 - Identification measures, (USB control etc.)
 - Identify key personnel within the company (including who the master reports suspected incidents to)
 - Identify key personnel within the company (including who the master reports suspected incidents to)
 - Hard copy of key contacts (e.g. DPA; CISO etc.)
 - Incident management record
 - Contractor compliance
 - Contractor compliance

- 7.15 Are the crew aware of the company policy on the control of physical access to all shipboard IT/OT systems?
- Note: Inspectors should observe if access to USB ports on 'shipboard IT/OT' terminals are controlled (i.e. there are measures in place to block/lock USB/RT45 ports on these terminals. Procedures should include the protection of critical equipment such as PCs from malware and virus attacks. Procedures should include the control of access to all shipboard IT/OT terminals including access to servers which should be in a secure location. The procedures should also include access by any third-party contractors and technicians.

- 7.16 Does the company have a policy or guidance on the use of personal devices onboard?
- Personal devices include phone/tablets etc and storage devices such as USB sticks.
- Check if the policy is implemented by both, crew and visitors, e.g. at third-party contractors and technicians.

- 7.17 Is Cyber Security awareness actively promoted by the company and onboard?
- Note: Examples of active promotion include:
- 'Cyber Awareness Material' displayed by all IT terminals and in crew rest rooms
 - Training films shown to crew
 - Crew specific training

© Copyright OCIMF 2019. All rights reserved.

VIQ 7.0.05 - 18 February 2019
74



Cyber Security in SIRE / VIQ 7

7.14 Are Cyber Security Policy and Procedures part of the Safety Management System and is there a Cyber Response Plan onboard?

Note: Do the procedures include a risk assessment of issues such as:

- *Threats such as from malware; phishing attacks etc.*
- *Identification and protection of Vulnerable systems (ECDIS etc)*
- *Mitigation measures, (USB control etc)*
- *Identify key personnel within the company (including who the master reports suspected incidents to)*
- *Hard copy of key contacts (e.g. DPA; CSO etc).*
- *Password management/record?*
- *Contractor compliance*

Note: Does the Cyber Response plan contain guidance on:

- *What 'symptoms' to look for,*
- *Immediate actions to be taken and*
- *Name, position, phone number and email for the Responsible Person to be contacted*



Cyber Security in SIRE / VIQ 7

7.15 Are the crew aware of the company policy on the control of physical access to all shipboard IT/OT systems?

Note: Inspectors should observe if access to USB ports on 'Shipboard IT/OT' terminals are controlled (i.e. there are measures in place to block/lock USB/RJ-45 ports on these terminals. Procedures should include the protection of Critical equipment such as ECDIS from malware and virus attacks. Procedures should include the control of access to all shipboard IT/OT terminals including access to Servers which should be in a secure location. The procedures should also include access by any third-party contractors and technicians.

7.16 Does the company have a policy or guidance on the use of personal devices onboard?

Personal devices include phone/tablets etc and storage devices such as USB sticks.

Check if the policy is implemented by both, crew and visitors, e.g. all third-party contractors and technicians.



Cyber Security in SIRE / VIQ 7

7.17 Is Cyber Security awareness actively promoted by the company and onboard?

Note: Examples of active promotion include:

- *'Cyber Awareness Material' displayed by all IT terminals and in crew rest rooms*
- *Training films shown to crew*
- *Crew specific training*
- *Instruction on safeguarding of passwords*
- *Responsible use of social media.*
- *Policy on the use of personal devices and its inclusion in shipboard joining familiarisation checklists.*
- *May include companies own employee/contractor Authorised User Policy (AUP) agreements.*
- *Company certified as per ISO 27001*

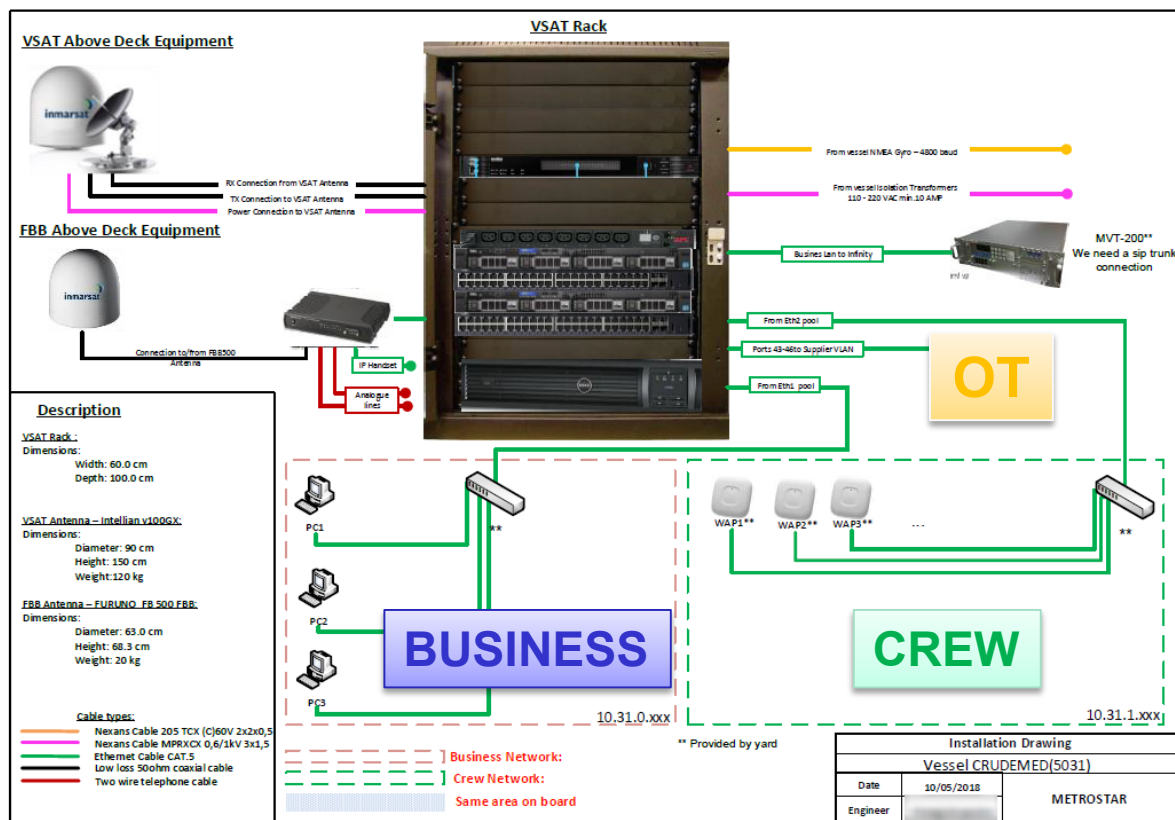


Key elements of our approach

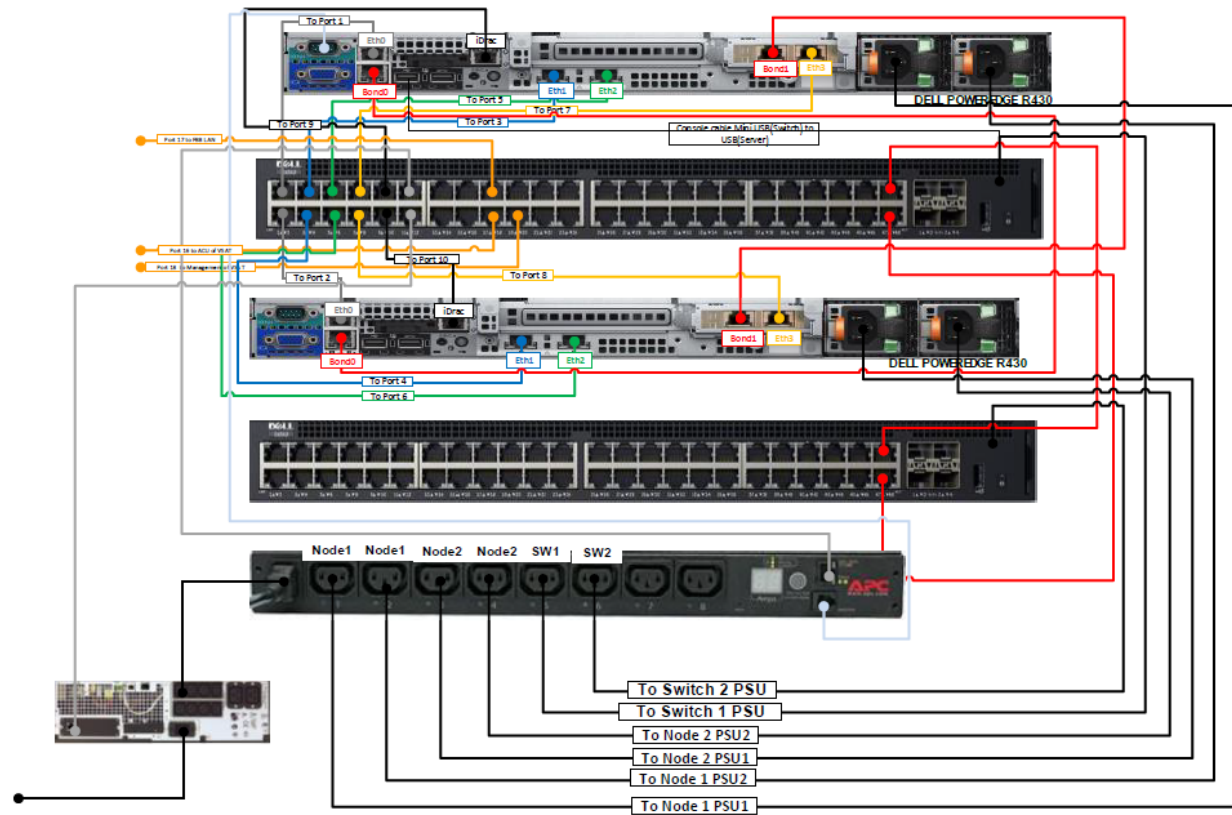
1. Extend our Cyber Security Policy to include both IT and OT equipment onboard
2. Logically and Physically separate IT & OT Networks
3. Introduce Cyber Risk Assessment & Change Management Procedure for IT & OT assets
4. Implement a USB Control Policy, enforced by hardware USB blocks and Safety Seals
5. Actively promote Crew Cyber Awareness



Network Segmentation



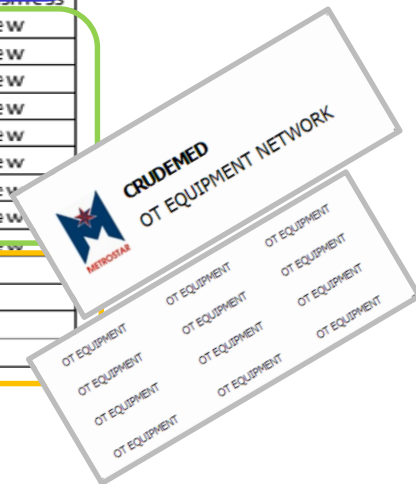
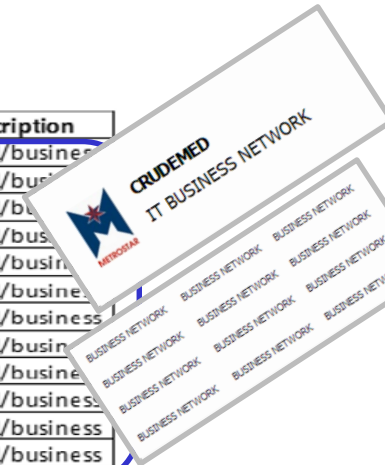
Network Segmentation (cont'd)



Network Segmentation (cont'd)



Vlan ID	Ports	Description
vlan10	21	eth1/business
vlan10	22	eth1/business
vlan10	23	eth1/business
vlan10	24	eth1/business
vlan10	25	eth1/business
vlan10	26	eth1/business
vlan10	27	eth1/business
vlan10	28	eth1/business
vlan10	29	eth1/business
vlan10	30	eth1/business
vlan10	31	eth1/business
vlan10	32	eth1/business
vlan10	33	eth1/business
eth2	34	eth2/crew
eth2	35	eth2/crew
eth2	36	eth2/crew
eth2	37	eth2/crew
eth2	38	eth2/crew
eth2	39	eth2/crew
eth2	40	eth2/crew
eth2	41	eth2/crew
eth2	42	eth2/crew
vlan11	43	vlan11
vlan11	44	vlan11
vlan11	45	vlan11
vlan11	46	vlan11





Risk Assessment & Change Management

VMS Vessel Risk Assessment IT Systems - Risk Report

[REFRESH](#)

ID	Asset Name-Primary Function	Impact Category - in case of failure	In the event of failure - do you know who to contact?	Is it connected to the Ships Network?	Does it have acces to Internet?	Is access to changing the configuration on this system restricted to authorised personnel?	Does this system have USB, DVD/CD Drives etc. ?	Risk
VMSstPC	Email PC-Email	Severe	Yes	Yes	No	Yes	Yes	Low
VMSstPC	Bridge PC-VMS	Minor	Yes	Yes	No	Yes	Yes	Very Low
VMSstPC	Chartco PC-Navigation	Severe	Yes	Yes	No	Yes	Yes	Low
VMSstPC	Master PC-VMS	Minor	Yes	Yes	No	Yes	Yes	Very Low
VMSstPC	Cheng PC-Shipsure	Severe	Yes	Yes	No	Yes	Yes	Low
VMSstPC	Choff PC-VMS	Minor	Yes	Yes	No	Yes	Yes	Very Low
VMSstPC	CCR PC-Shipsure	Minor	Yes	Yes	No	Yes	Yes	Very Low
VMSstPC	ECR PC-Shipsure	Minor	Yes	Yes	No	Yes	Yes	Very Low
CLC-CM	Cargo Loading Computer-Cargo Management	Major Cargo Impact	Yes	No	No	Yes	Yes	Low
CMS	TANK LEVEL AND TEMPERATURE GAUGEWITH TANK PRESSURE GAUGE-Cargo Management	Major Cargo Impact	Yes	No	No	Yes	Yes	Low
MPMS	CARGO MANIFOLD PRESSURE MONITORING SYSTEM-Cargo Management	Moderate	Yes	No	No	Yes	Yes	Very Low
BWTS	BALLAST WATER TREATMENT SYSTEM-Cargo Management	Major Cargo Impact	Yes	No	No	Yes	Yes	Low
ODME	OIL DISCHARGE MONITORING SYSTEM-Cargo Management	Severe	Yes	No	No	Yes	Yes	Low
WAS	WIND ALARM SYSTEM-Cargo Management	Minor	Yes	No	No	Yes	Yes	Very Low
CNS	Computer Network Server-Systems network	Minor	Yes	Yes	No	Yes	Yes	Very Low
ECDIS	ECDIS-Navigation	Severe	Yes	No	No	Yes	Yes	Low
Radar	Chart Radar-Navigation	Severe	Yes	No	No	Yes	Yes	Low
EMC	Engine Management Computer-Machinery/Power Control	Minor	Yes	No	No	Yes	Yes	Very Low
Aconis	Alarm Monitoring Computer-Other	Minor	Yes	No	No	Yes	Yes	Very Low
MOP	EC MOP-Other	Minor	Yes	No	No	Yes	Yes	Very Low
GPS	GPS-Navigation	Severe	Yes	No	No	Yes	Yes	Low
AIS	AIS-Navigation	Minor	Yes	No	No	Yes	Yes	Very Low
GMDSS	GMDSS-Communications	Moderate	Yes	No	No	Yes	Yes	Very Low
VDR	VDR-Other	Minor	Yes	No	No	Yes	Yes	Very Low
CD	CONNING DISPLAY-Navigation	Minor	Yes	No	No	Yes	Yes	Very Low
BNWAS	BNWAS-Navigation	Moderate	Yes	No	No	Yes	Yes	Very Low
SSAS	SSAS-Communications	Critical	Yes	No	No	Yes	Yes	Medium
CCTV	CCTV-Other	Moderate	Yes	No	No	Yes	Yes	Very Low
FBB	FBB-Communications	Moderate	Yes	No	No	No	No	Very Low
SATC	INMARSAT C-Communications	Moderate	Yes	No	No	No	Yes	Low

USB Control Policy



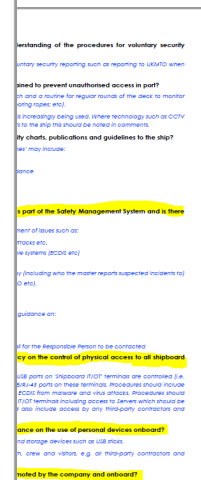
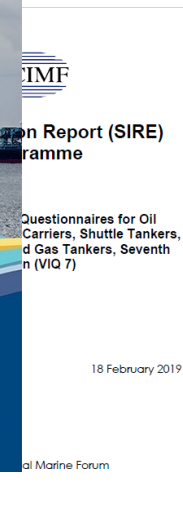
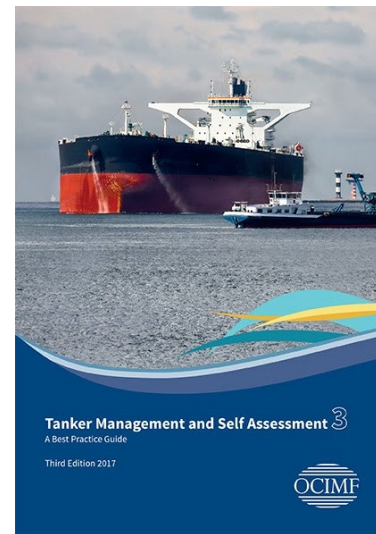
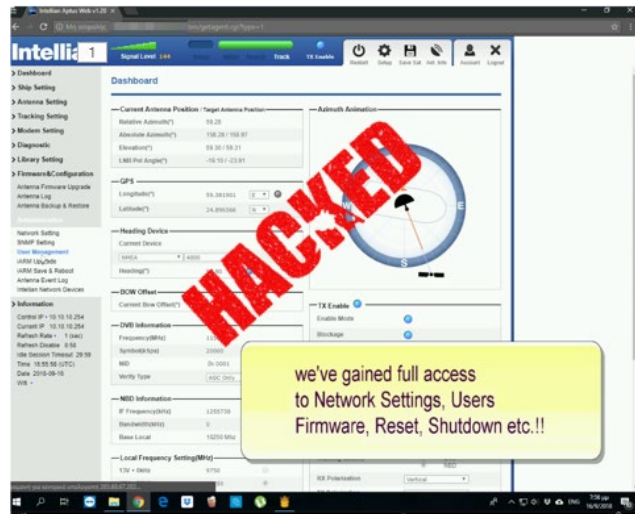


Conclusion & lessons learned

We are facing two kinds of risks:

1. Operational & Reputational Cyber Risk (CIA, Fraud)
2. Compliance Risk (TMSA 3 / VIQ 7, GDPR, IMO)

We need to stay ahead of the curve on both fronts!





Digital Ship



ATHENS, 7 MAY 2019

Dr. Matthew Maheras
IT Manager
Metrostar Management Corp.