

A hand in a dark suit jacket is pointing towards a digital interface. The interface features several icons and text elements: three interlocking gears, a bar chart, a padlock, a network diagram, and a trash can. Text elements include 'Innovation Branding Solution Marketing Analysis Ideas Success Management', 'INDUSTRY', 'Manufacturing Supply chain Product Cargo Customer Delivery Inventory Management Freight', and 'ment'.

Speakers'  
Presentations &  
Event Photographs

Thank you  
for joining  
us at

2017  
Ship Owner  
Seminar  
Hong Kong

20th November 2017

[ship-owners.com](http://ship-owners.com)

# Why?

The Hong Kong Ship Owner Seminar aims to build new and strengthen existing relationships with C-level ship owner executives in the region.

The goal is to offer a programme that addresses the challenges and effects that new data-centric and connected technologies have on the C-suite and boardroom agendas of the Asian shipping community.

Part 1 of the seminar will focus on the high cost of mistakes and non-compliance and the significant benefits to be gained when doing it right. By demonstrating a hands on approach to discussing and developing solutions that meet today's shipping business challenges, we are able to establish an arena for useful discussions around how the digital world affects us today, and tomorrow.

Part 2 will consist of an interactive session presenting the different innovations Marlink and partners have available such as telemedicine, remote IT support, e-learning on-board, e-navigation and satcoms. Guests can mingle from demo station to demo station and benefit from a nice networking arena among other senior decision makers.



## Organised by



Marlink is the pioneer of business critical communication solutions for customers operating in remote environments. With 600 employees and 27 offices worldwide, the company is the largest technology-independent satellite communication and digital solutions provider serving the maritime and enterprise markets. Marlink's multi-band communication services covering Ku, Ka, C and L-band extended with mobile and terrestrial links, enable over 200,000 customers to operate in an ever smarter, safer and more profitable way.

With over 75 years' experience in developing innovative business critical communication solutions, Marlink's strategy is to deliver the benefits of a digital and connected world to its customers' remote operations. Today Marlink is the leading maritime communication and VSAT operator in the world. Marlink leverages strong partnerships with all major satellite network operators to deliver communication solutions direct to the customer and via an unrivalled network of service provider partners.



[marlink.com](http://marlink.com)

[telemarhk.com](http://telemarhk.com)



## Contributor

### Opening Remarks - HKSOA Speaker

The Hong Kong Shipowners Association was incorporated in 1957 by 11 local shipowners with the purpose of creating a forum for shipowners resident in Hong Kong. Over the past 60 years, the Association has grown into one of the world's largest Shipowner Associations, its members owning, managing and operating a fleet with a combined carrying capacity of over 178 million deadweight tonnes.



[hksoa.org](http://hksoa.org)

## Agenda

13.30 hrs - Registration opens with coffee and tea.

14.00 – 14.10 hrs  
Opening remarks - HKSOA.

14.10 – 14.20 hrs  
CBA's innovation lab and other functions of CBA.

14.20 – 14.45 hrs  
GDPR – From reactive to proactive data protection.

14.45 – 15.10 hrs  
Blockchain and how it will affect Asian Ship Owners.

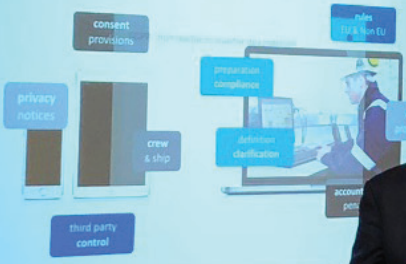
15.10 – 15.35 hrs  
Cyber risks, a new challenge for classification societies.

Coffee break – 35 minutes.

16.10 – 16.25 hrs  
How to save money, time and stay in compliance with IT and comms.

16.25 – 18.10 hrs  
Demo stations experiences and networking.

SHIP GROUP SEMINAR  
GDPR - from reactive to proactive data protection



GDPR is a  
GDPR DNA





# Moderator

## Neville Smith

Director, Mariner  
Communications

Neville Smith is a maritime media consultant with shipping industry clients across communications, navigation, IT and marine products and services.

A maritime journalist for 16 years and a former deputy editor of daily maritime newspaper Lloyd's List, he works for clients on messaging, positioning and campaign delivery across print and electronic media as well as blogging on current and future trends in communications and technology.

[maritimeinsight.com](http://maritimeinsight.com)



**HFW**

# THE EU GENERAL DATA PROTECTION REGULATION (GDPR) IN APAC: WHAT DOES IT MEAN FOR YOU?

**FROM REACTIVE TO PROACTIVE**  
Hong Kong – 20 November 2017

Scott Pilkington, Partner  
T: +85 6411 5357  
scott.pilkington@hfw.com

*Only 186 working days until the GDPR comes into force in May 2018*



# GDPR

## From reactive to proactive data protection

With penalties of up to 4% of turnover (not profit!) for non-compliance, the EU General Data Protection Resolution (GDPR) comes into force on 25th May 2018.

It covers EU registered vessels but also any companies that offer goods and services to EU citizens, making it vital that Asian ship owner executives understand the consequences of not securing their data.

- How will GDPR affect ship owners in general?
- How should Asian ship owners react to it and what can they do to prepare?
- What are the consequences of not complying in time?



## Scott Pilkington

Partner, HFW (Singapore Office)

Scott acts for clients in the maritime, offshore and commodities sectors. He has a broad practice in maritime and international trade disputes, and also has particular experience of the container liner supply chain, having previously worked for the UK's leading ship manager of container vessels, and also of wet and dry bulk carriers and car carriers.

Scott has worked on numerous high profile casualties, including collisions, groundings, total losses, and fires at sea. He advises on insurance matters and has particular experience of offshore disputes, involving OSVs and PSVs and tug and tow.

He spent time on secondment for a large insurance company in Japan. Scott's time on secondments gives him practical and commercial understanding.



Scott lectures frequently, including for leading industry groups and training providers.



*HFW*

# THE EU GENERAL DATA PROTECTION REGULATION (THE GDPR) IN APAC: WHY COMPLY ?

FROM REACTIVE TO PROACTIVE  
Hong Kong – 20 November 2017

Scott Pilkington, Partner  
T: +65 6411 5357  
E: [scott.pilkington@hfw.com](mailto:scott.pilkington@hfw.com)

*Only 186 working days until the GDPR comes into force in May 2018*



1. WHAT IS IT?

2. WHAT'S NEW,  
AND WHAT DOES  
IT DO?

3. WHY SHOULD  
YOU CARE?

4. WHAT MUST  
YOU DO?

---

HFW

# 1. WHAT IS THE “GDPR”?

Regulation (EU) 2016/679 “*on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*”

Comes into effect on 25 May 2018

Data Subject's rights

Natural persons – whatever their nationality or place of residence

Duty to notify any breach

Extra territorial effect

Controllers and Processors

Data protection impact assessment

---

1. Are any of your vessels flagged within the EEA?

2. Is your website directed towards customers based in the EEA, for example by using an EEA currency, or a particular language?

3. Can your services be bought from within the EEA?

4. Do you have a registered establishment or an office in the EEA?

---

5. Is your business currently registered with an EEA data protection authority?

6. Do you use servers located in the EEA?

7. Do you monitor the behaviour of any individuals within the EEA (irrespective of their nationality or habitual residence)? For example, if your website uses tracking cookies, then you are “monitoring individuals” for the purposes of the GDPR.

If the answer to any of these questions is ‘yes’ then it is likely that the GDPR applies to you.

---

HFV

## 2. WHAT'S NEW, AND WHAT DOES IT DO?



## THE GDPR IS THE BIGGEST SHAKEUP OF DATA PROTECTION LAW IN 20 YEARS

This landmark piece of legislation will impact every entity that holds or uses European personal data.

**1. Heavy financial penalties for breaches**

**2. Overall increased focus on operational adequacy and accountability**

**3. New and enhanced citizens' rights**

**4. Mandatory breach disclosure**

**5. Sets up possible US-style class action for privacy breaches**

...and even the definition of 'personal data' has changed...

---



**THIS IS A SIGNIFICANT STEP UP FROM THE EXISTING PRIVACY REGULATION**

**Understand the data they hold and how they use it.**



**A new “Transparency Framework”**

**Clear compliance steps to be taken, evidence of this is essential.**



**A new “Compliance Journey”**

**Reputation risk: non compliance fines and the potential for litigation and class action.**



**A new “Punishment Regime”**



CONTROLLERS, PROCESSORS AND PROCESSING

Controller:	Processor:	Processing:
<p><i>“the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data”</i></p> <p>the Controller shall implement <u>appropriate technical and organisational measures</u> to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary. (art. 24.1)</p>	<p><i>“a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”</i></p>	<p><i>“any operation ...which is performed on personal data...,whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alternation, retrieval, consultation, use disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”</i></p>

## Personal Data (Article 4)

- **Any information relating to an identified or identifiable natural person;** an identifiable natural person ... can be identified, directly or indirectly... by reference to an **identifier** such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”
- Only relates to **living** individuals (as with current law)
- Includes e.g. business emails and browsing history

## Special Categories of Personal Data (Article 9)

- Very similar to current law on “sensitive personal data” but updated
  - Includes personal data **revealing** racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, health data, sex life or sexual orientation
  - Data on criminal convictions and offences treated under different laws
-

- Additional and enhanced individuals' rights including:

Right to object to processing access

Right to restrict processing (e.g. not for direct marketing)

Right to erasure (existing "right to be forgotten" right codified)

Not an absolute right, must have valid reasons, e.g. data no longer necessary for the purpose collected or withdrawal of consent.

Continued...

Right to forbid  
profiling  
which results in  
significant  
decisions

Right to data  
portability

Enhanced  
subject access  
rights  
(entitled to more  
information)

- where processing  
electronic and  
grounds for  
processing are  
consent or contract

40 day  
response  
window

---

- **New focus on accountability – must keep records of processing**
  - **Enhanced transparency requirements:**
    - **Privacy notices will need updating**
    - **Individuals must be notified when their data is received from third parties.**
  - **Additional data breach reporting requirements**
  - **Contracts with processors**
    - ***New elements must be included***
-

HFV

# 3. WHY SHOULD YOU CARE?

- Potential fines of up to 4% of global turnover or €20 million (whichever is the greater)
  - Risk of legal challenge from individuals / class actions (enforcement/compensation)
  - Reputational damage
  - Affects cross border business
  - Customer pressure
-



**'Personal data breach'** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Name, date of birth, family details (including children), medical records and other possibly sensitive information. Duty to protect, whether transmitting, *storing* or processing

Duty to notify the supervisory authority in the event of breach within 72 hours or "without delay"

Have you been "hacked"?

---

HFw

# 4. WHAT MUST YOU DO?





## WHEN CAN YOU PROCESS PERSONAL DATA?

Grounds for processing similar to current law – at least one of :

1. Consent of the data subject (for the particular purpose)
  2. Necessary for the performance of a contract **with data subject**
  3. Necessary for compliance with a legal obligation
  4. Necessary to protect “vital interests” of data subject/third party
  5. Necessary for performance of a task in the public interest
  6. Necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party (balancing exercise of rights) – BUT, except where overridden by the interests or fundamental rights and freedoms of the data subject
-

- “Consent” definition made stricter

...freely given, specific, informed **and unambiguous** indication of the data subject’s wishes by which he or she **by a statement or by a clear affirmative action** signifies agreement ...

- No implied consent
-

- Additional clarifications / obligations under GDPR:

Controller must be able to <b>demonstrate</b> that data subject has consented	Must have right to withdraw consent at any time
Where consent part of written declaration also concerning other matters, consent element must be clear and user friendly or not binding	Consent may not be “freely given” if performance of contract conditional on consent

- Consent no longer an “easy” legal ground for processing
-

1. Data audit:-

- What personal data do you hold and what for (especially with regard to “sensitive” data)
- Document findings and decisions

2. Draft or amend policies and procedures

- To deal with any breach, including reporting it without delay/within 72 hours
- When and how to conduct privacy impact assessment
- Record-keeping

3. Inform individuals about processing

- Check and update existing draft privacy notification forms or draft new ones

4. Amend or put contracts in place with data processors – indemnities...

5. Appoint a data protection officer?

- Do you need to? May choose to do so voluntarily, given the increased risks involved.

*HFW*

**“BY DESIGN AND  
BY DEFAULT”**

**“Data Minimization”**

*“The Controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to:*

<p><b>the amount of personal data collected</b></p>	<p><b>the period of their storage; and</b></p>
<p><b>the extent of their processing</b></p>	<p><b>their accessibility</b></p>

*In particular such measures shall ensure that by default personal data are not made accessible without the individual’s intervention to an indefinite number of natural persons.”*





## THE GDPR 'LEGISLATIVE COMPLIANCE JOURNEY'

The GDPR defines a 'compliance approach' through the full lifecycle, from data analysis to dealing with failures.

1. Analyse	What data will you process, how and why? [A.22]
2. Risk assess	What are the risks and what harms can be caused? [A.33]
3. Consult	Which stakeholders do you need to consult with? [A.34]
4. Design	How will you build in data protection from the beginning of processing? [A.23]
5. Document	How will you prove compliance? [A.7,8,22,28]
6. Engage	What information should you give to the public and what consents do you need? [A.7,8,12,14]
7. Challenge	How will you handle incidents, problems and complaints? [A.31,32]
8. Supervision	How will you handle the use of legal rights and supervisory powers? [A.15,16,17,18,19,52,53,73]
9. Sanctions and litigation	How will you cope with the most serious regulatory sanction and civil litigation? [A.75,77,79]

### KEY ELEMENTS THAT THE REGULATORS WILL EXPECT

- an organisational view on what Privacy means to you
  - a clear understanding of what data is held, why you have it, where it is and who has access to it
  - understand and manage the risks introduced to the data by third parties
  - Privacy model is designed with agility in mind given the ever changing Privacy landscape
  - understand how Privacy and Data Protection fit into your overall business strategy
  - know how well you are protecting the data, and where you are not
  - using the data for the purpose that you have committed to and nothing more
  - help to empower individuals, so they can control the use of their data better
-

1. WHAT IS IT?

2. WHAT'S NEW,  
AND WHAT DOES  
IT DO?

3. WHY SHOULD  
YOU CARE?

4. WHAT MUST  
YOU DO?

---



HFW

**Thank you**

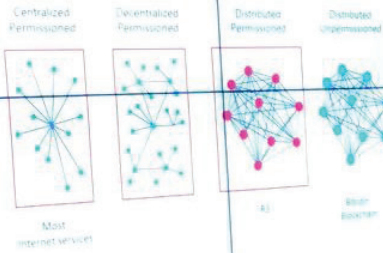
Scott Pilkington, Partner

T: +65 6411 5357

E: [scott.pilkington@hfw.com](mailto:scott.pilkington@hfw.com)

*Only 186 working days until the GDPR comes into force in May 2018*

# Blockchain Network



# Blockchain

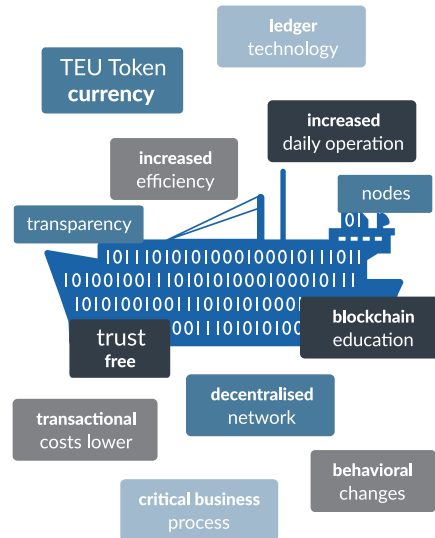
## And how it will affect ship owners

With blockchain technology, the number of stakeholders in a transactional process can be reduced, lowering costs, delays and complexity.

Likewise, a new crypto currency called TEU has been designed to be a more efficient platform for trading containers.

How can Asian ship owners navigate a path to leverage this powerful new technology for business growth and efficiency?

- How will blockchain and crypto currency change the way we interact in shipping?
- Are Asian ship owners ready for more transparency and trust?
- How will the industry look if fewer agents, ship brokers and other middlemen are required?
- How can ship owners save money and become more efficient by implementing blockchain?



# Johnson Leung

## Co-founder 300 Cubits

Johnson comes from a traditional shipping background where he spent the first seven years of his career with Maersk Line in Denmark, Brazil and China before working for Hutchison Port Holdings as an Investment Manager specializing in acquiring and negotiating port concessions in the Middle East.

Johnson's last assignment with Maersk was the eCommerce project at headquarters, where he provided business logic for the development of Maersk Line's on-line platform, similar to our TEU Ecosystem. Moving from industry to finance, he was the regional shipping analyst at JP Morgan and then a senior shipping analyst for Tufton Oceanic, the largest shipping hedge fund, before joining Jefferies as their Head of Regional Transport and Industrials Research for the Asia Pacific region.



Johnson is a graduate of Maersk Shipping Academy and HKUST, and holds an INSEAD MBA.



# 300cubits

**TEU – A Bitcoin for Shipping**  
20 Nov 2017



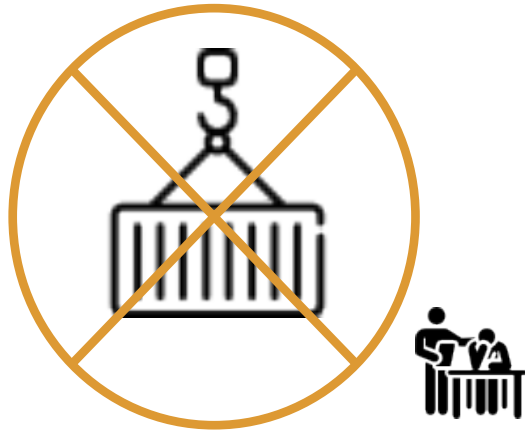
# **TEU Token**

## **A Bitcoin For Shipping**





# Broken Booking And Solutions In Market

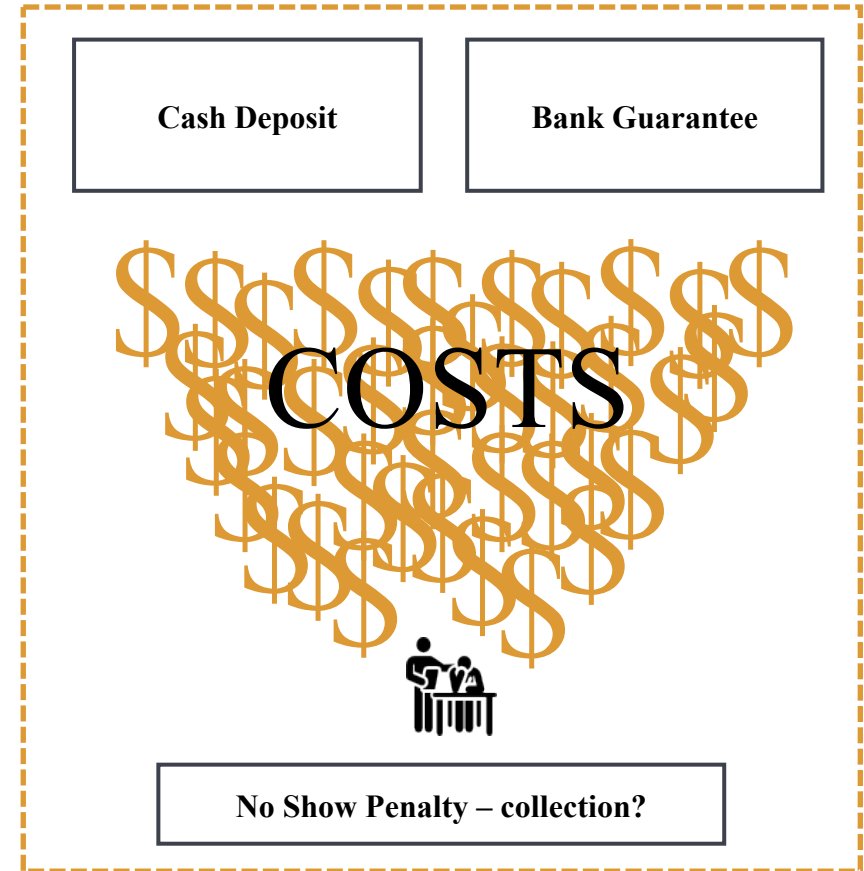


Wastage: **\$23bn** p.a.

**Liners' complaint:** 5-20% bookings never show

**Customers' complaint:** both contracted shipments and spot shipments are frequently rolled

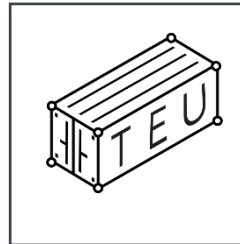
## Server vs Blockchain Based



Source: NJIT, Hapag Lloyd

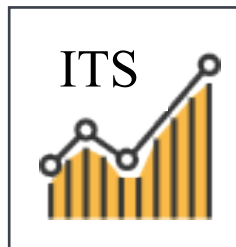


# Creation of bitcoin for shipping - TEU



100mn TEU tokens minted

**Token  
Minting**



2mn TEU tokens sold at Pre-Sale  
18mn TEU tokens to be sold at ITS

**Value  
Creation**

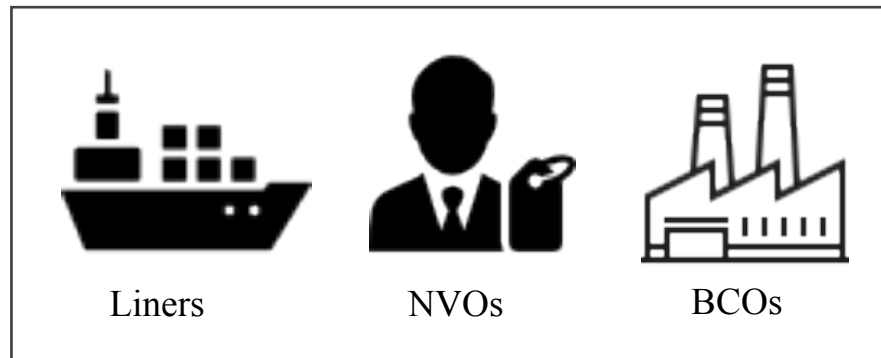
TEU tokens listed in exchanges



Crypto Market



[54]mn TEU tokens given to industry



Liners

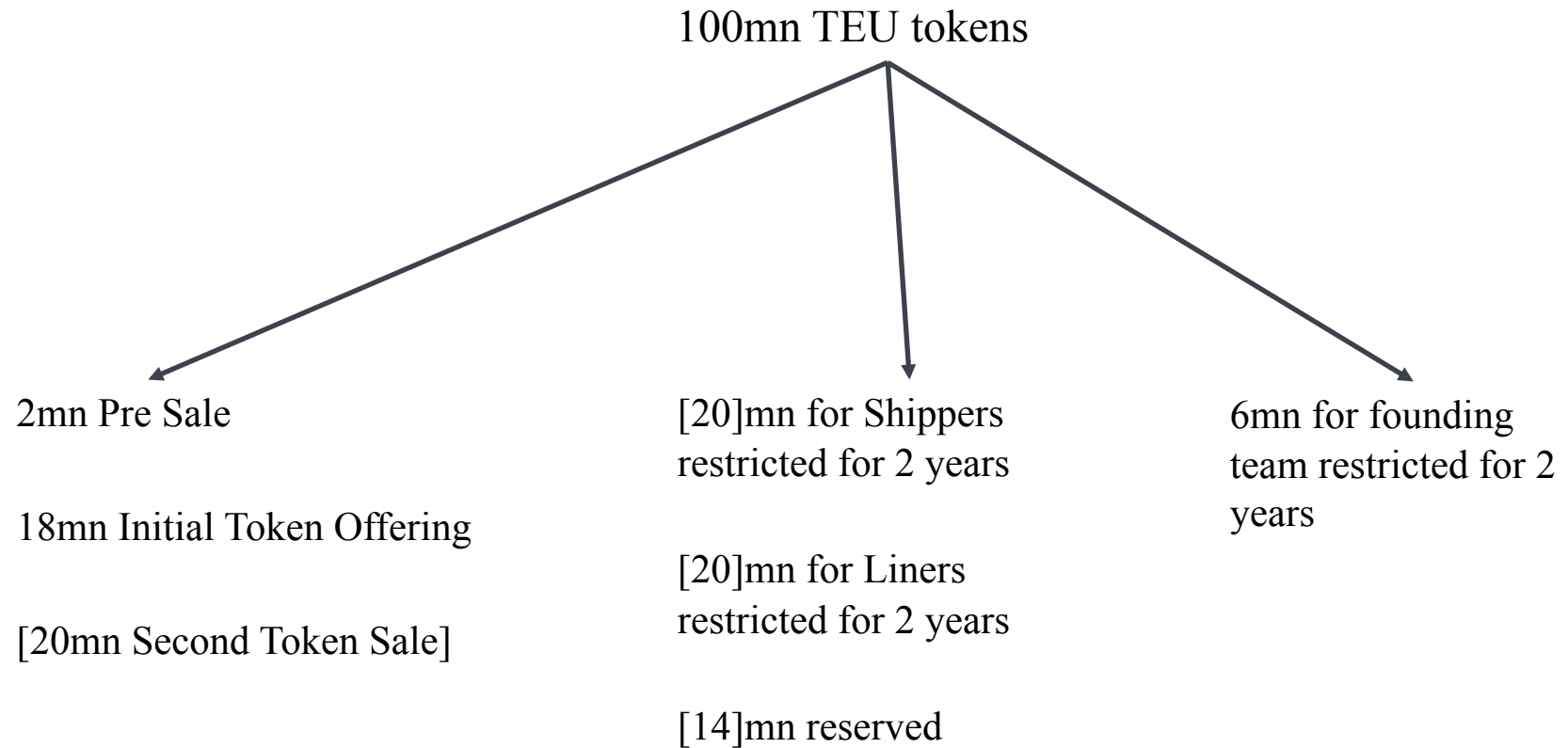
NVOs

BCOs

**Value  
Enhancement**



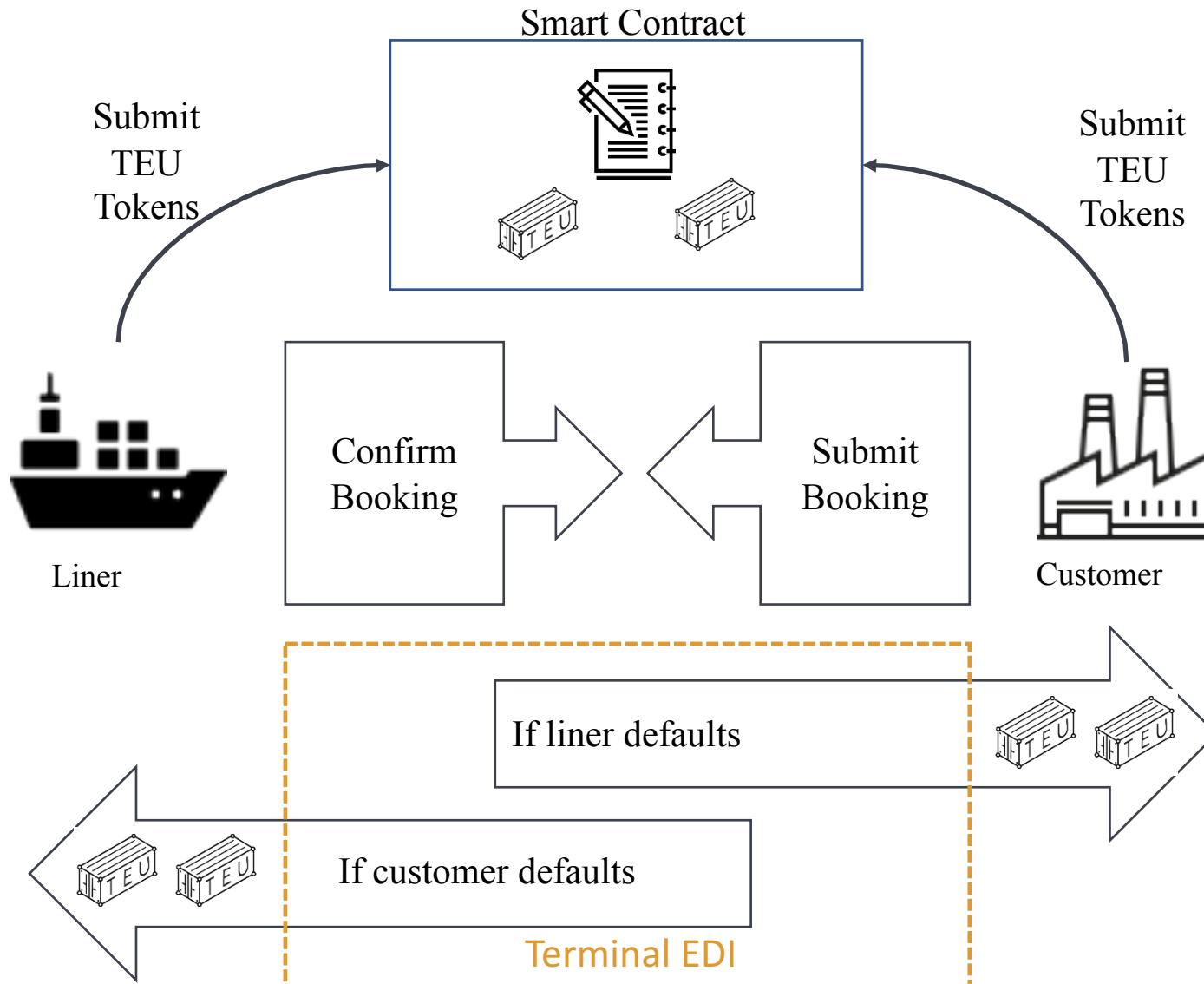
# Token distributions



Note: [\*] are figures and event subject to changes

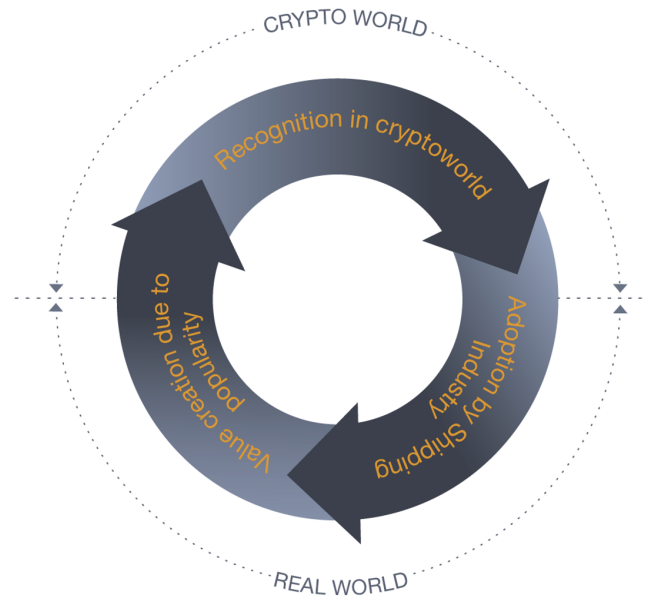


# How TEU Works? Booking Deposit





# Value Creation and Propositions



Benefit for society:

- Reduction of wastage
- Sustainable supply chain
- Re-allocation of capital

Benefits for crypto world:

- First token used in real world
- Value appreciation

Benefits for industry:

- Value injection
- Value appreciation
- Solution for industry pain points

In a blockchain, the solution

- peer-to-peer, secure and trust free: removal of reliance of middleman and middleman's counterparty risk
- open-sourced: free for all liners, freight forwarders and common booking portals to adopt the solution



# Project Roadmap: main milestones ahead



Oct/Nov 2017 enter MOU with **industry players** for collaboration

Nov 2017  
Completion of development for **Master Booking Smart Contract**



Jun 2018 **Booking Module** go live

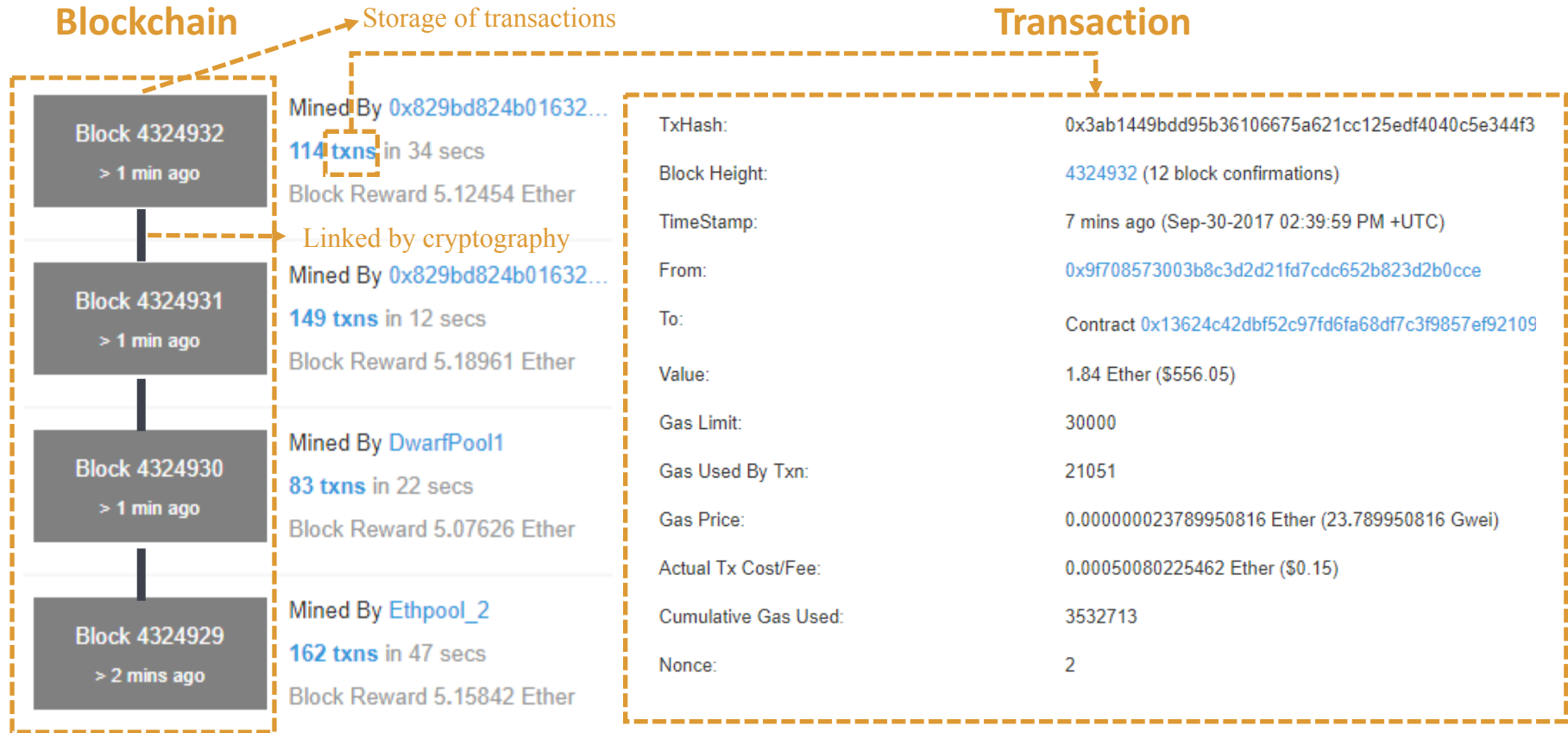




# Blockchain & Crypto Currencies



# Blockchain: High Level View



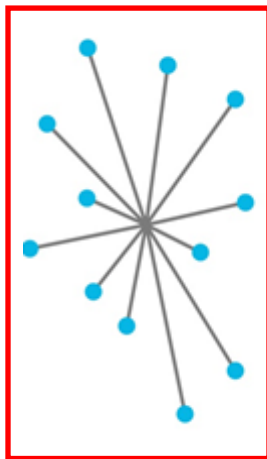
- Essentially, the blockchain is just a distributed database with certain useful characteristics
- The block: A batch of transactions
- The chain: Integrity is ensured by cryptography





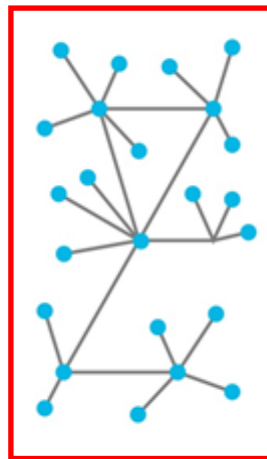
# Blockchain Network

Centralized  
Permissioned

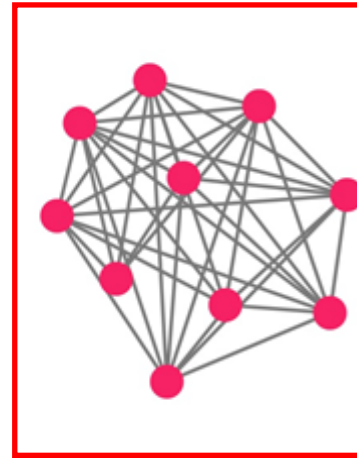


Most  
Internet services

Decentralized  
Permissioned



Distributed  
Permissioned



R3

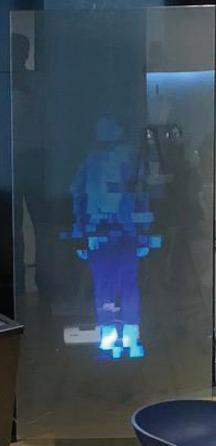
Distributed  
Unpermissioned



Bitcoin  
Blockchain

Source: blockgeeks

Safety Moment



# Cyber Risks

## A new challenge for classification societies

As vessels become more connected in the drive towards smarter shipping, Classification Societies are responding to the challenge of cyber risks and providing support for owners that extends beyond the traditional class remit.

- What are the main factors driving the shipping operators to improve their cyber protection?
- How do you protect the connected ship?
- What can owners do to adopt a proactive cyber policy?



## Pier Carazzai

### Hong Kong Area Manager, ABS

Pier Carazzai serves as Area Manager covering the offices of Taiwan, Hong Kong and the District of ABS South-eastern China which includes Guangdong Province, Guangxi Province and Hainan Island. Pier was named to his current position in November 2016, after being General Manager of ABS Hong Kong office from March 2014.

Prior to this roles he served as Director of Engineering at ABS London and Manager of the Technical Consistency Department at ABS' Corporate Headquarters in Houston, Texas-USA.

As Director of ABS London engineering, from 2009 to 2014, Pier had oversight of 80+ engineers and the administrative staff involved in shipping, offshore and vendors project throughout the Europe Division.



Pier graduated from the University of Genoa (Italy) with a degree in Naval Architecture and Marine Engineering in 1995, he also became a Chartered Engineer.



# Cyber Risk

## A new challenge for Classification Societies

---

Pier Carazzai | 20 November 2017  
Hong Kong



© 2017 American Bureau of Shipping. All rights reserved

---

# Safety Moment



# Cyber Risks in the era of SMART vessels

What are the main factors driving the shipping operators to improve their cyber protection?

What can owners do to adopt a proactive cyber policy?

How to you protect a connected ship?

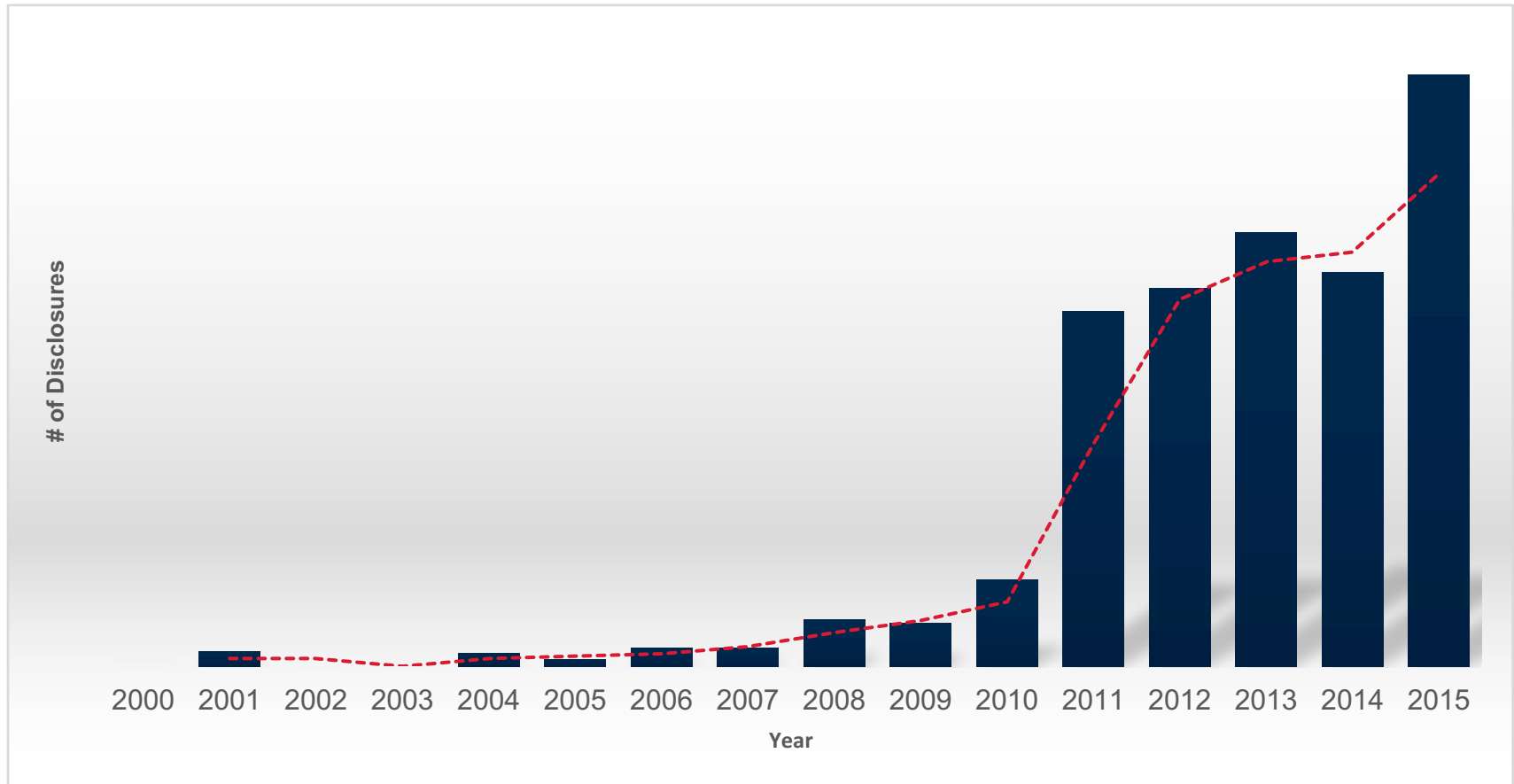
---

# Driving Factors

- USCG Policy Letter – 14 December 2016
- IMO MSC (98) – Specific Procedure ISM Code 2021
- TMSA 3 Compliance for Cybersecurity - 2018
- Oil Majors adding CyberSafety elements to vetting inspections
- BIMCO- Intercargo-Intertanko – June 2017
- Marine insurance Cyber exclusion clause
- Increase in cyber-related maritime incidents
- SmartShip Technology
- Data-Centric Asset

---

# Control System-Specific Vulnerability Disclosure



- People are looking for OT vulnerabilities since Stuxnet attack on Iran (Siemens Step 7)
  - The statistic is sourced from the 2016 industrial control systems (ICS) vulnerability trend report, by Fireeye iSight Intelligence



# Smarter ships....more automation....more connections ...

## Machinery Systems

- Design for unmanned operation
- Control systems, condition monitoring, condition based maintenance
- Short sea shipping: electrical propulsion, battery powered

## Navigation and collision avoidance

- Steering capability
- Weather monitoring and routing
- Automated collision avoidance systems

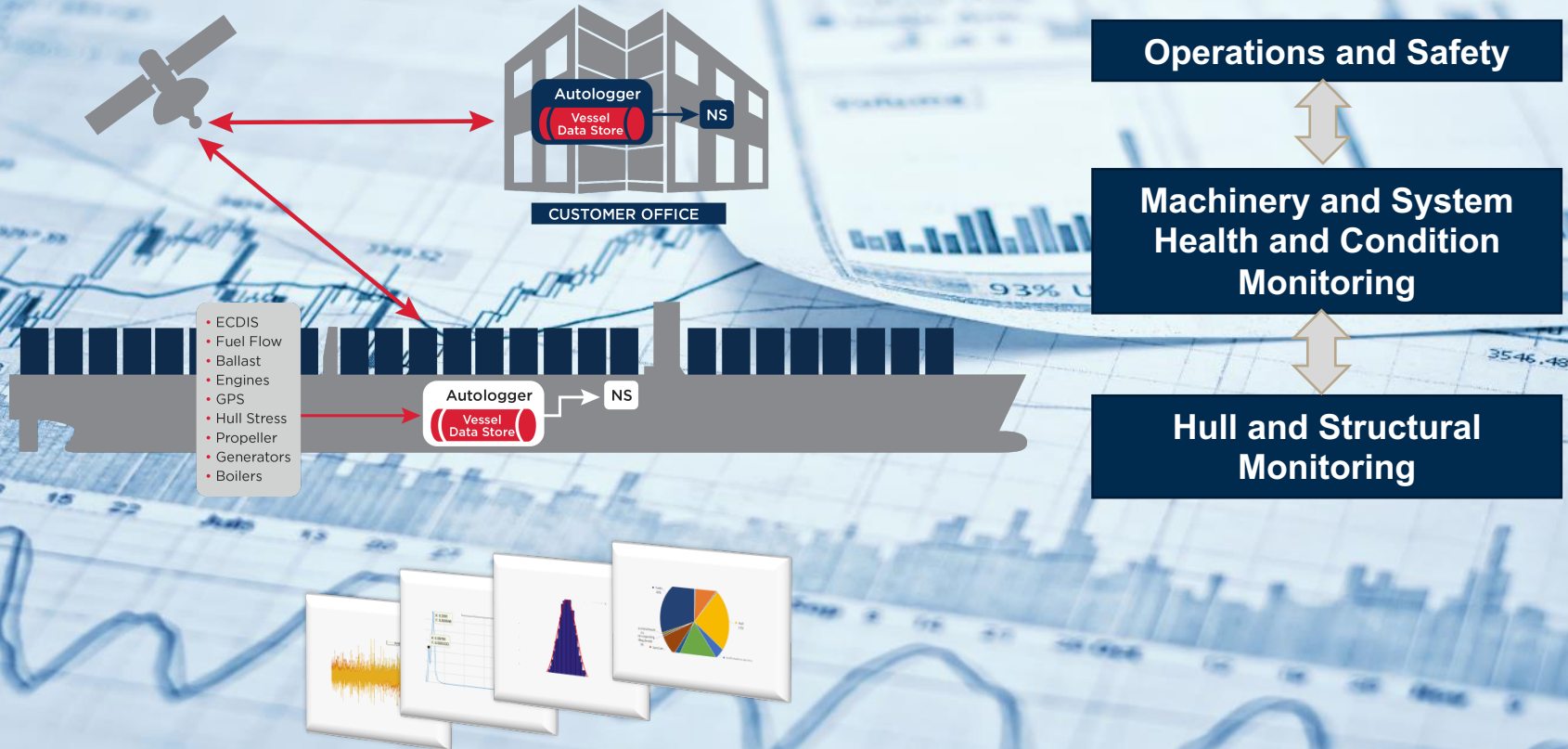
## Data Handling

- Sensors, data collection and transmission
- Connectivity, satellite systems, time analysis
- Storage



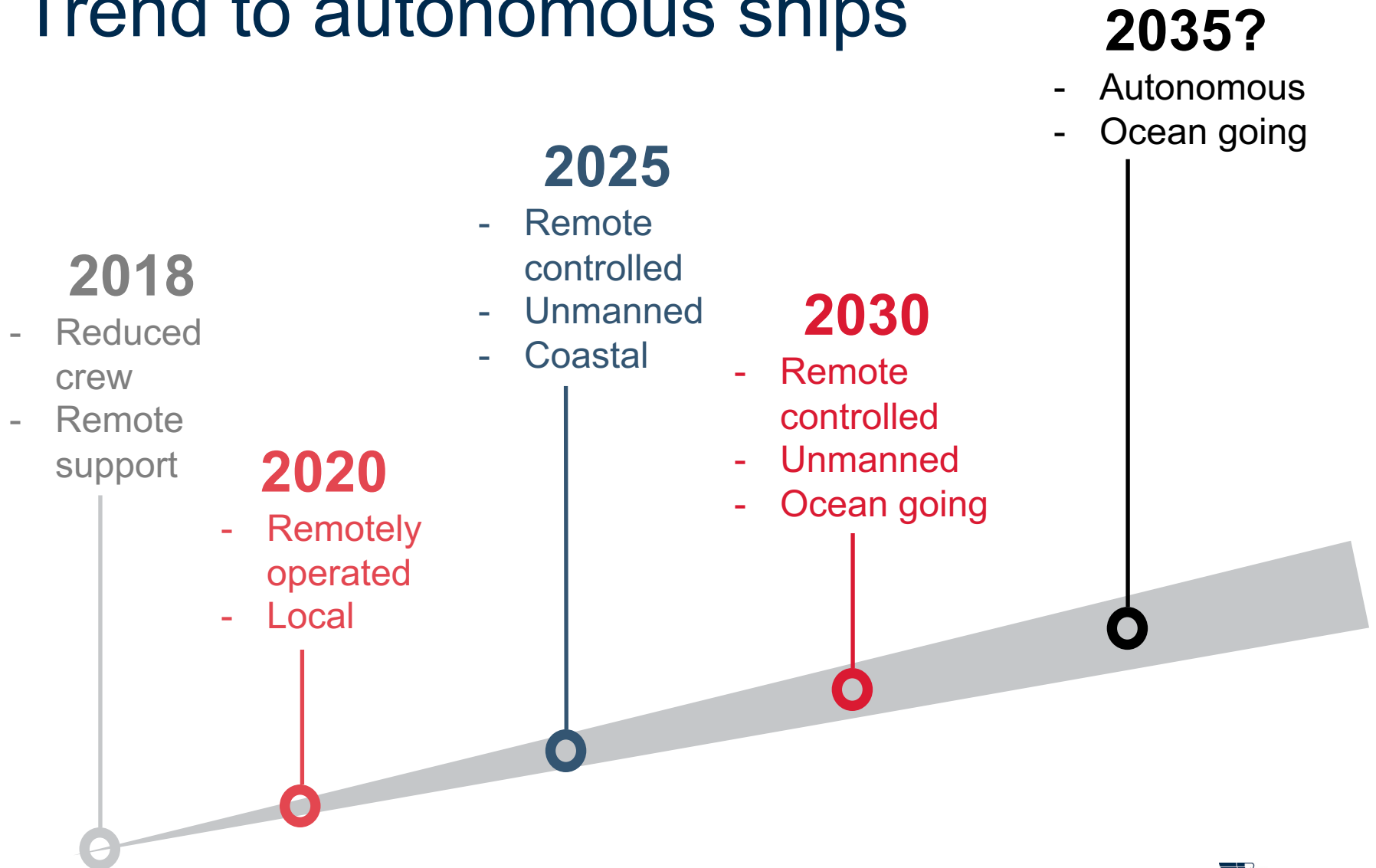
© archy13/Shutterstock

# Data-Centric Asset

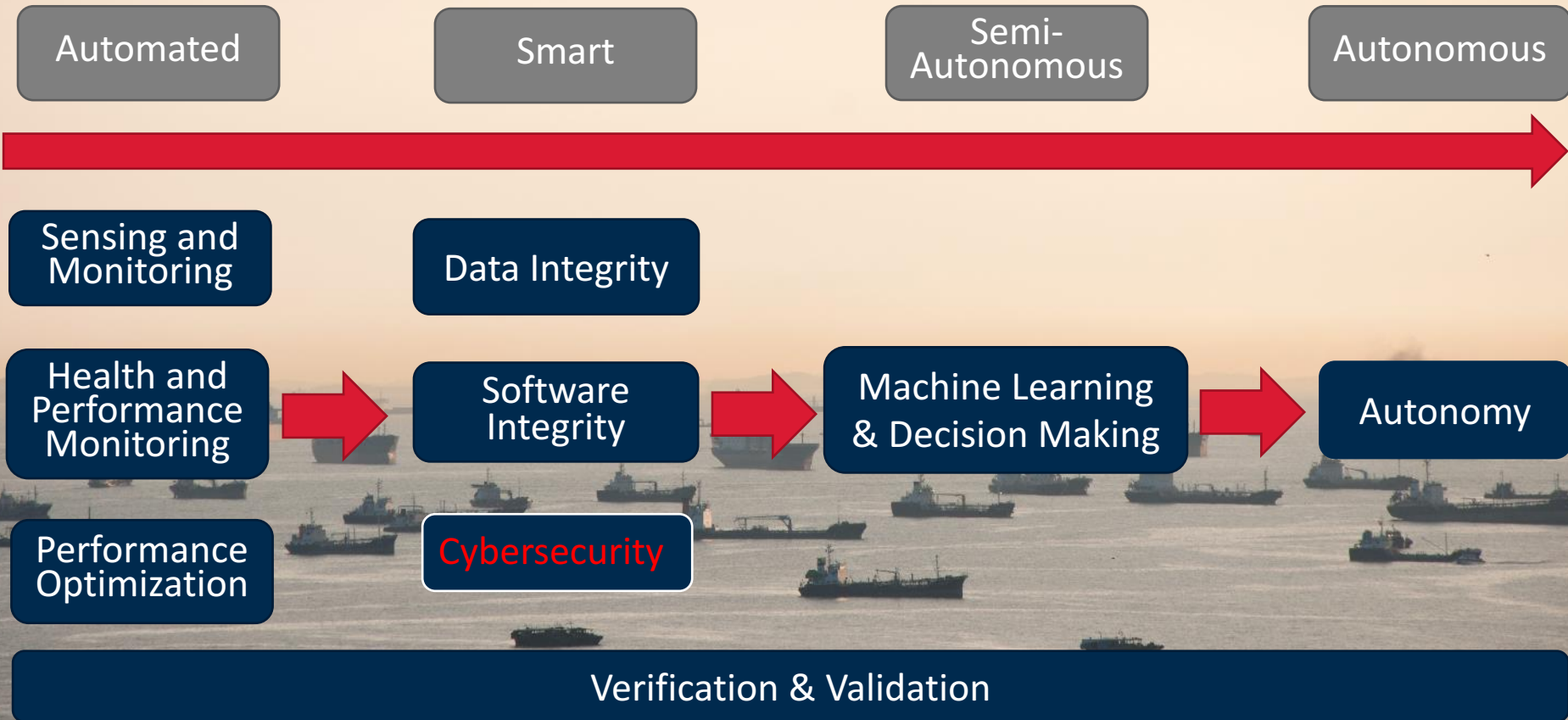


© Alzay/Shutterstock

# Trend to autonomous ships



# Long journey from Smart to Autonomous... Cyber Protection is needed from now on.....



© /Shutterstock

---

# Basic Questions to start with

- Who manages your OT systems and software upgrades?
- Do you have basic policies in place to upgrade systems?
- Are you formally tracking software version control?
- Is Cyber part of your safety culture onboard the vessels?
- Do you have examples of failed software upgrades?

.....better to perform an assessment .....

---

# Value Proposition

The ABS CyberSafety® program identifies risks and increases awareness of and protection from cyber threats to:

- Enhance safety
- Minimize productivity loss
- Limit operational impact

- Only 38% of global organizations claim they are prepared to handle a sophisticated cyberattack
- Industrial Control System (ICS) specific vulnerability disclosures will increase over the next years at a 5% rate
- Distinct risks in the marine environment have serious consequences
- Most cyber-related threats are preventable with the right risk-based approach and systems in place

# ABS Experience

ABS awarded research contract by the Maritime Security Center (MSC) to lead industry partnership to determine direction of cybersecurity 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 cybersecurity posture of the MTS enterprise.”

- Dr. Hady Salloum  
Director of MSC

## 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

CYBERSECURITY ASSESSMENT OF  
**30+** MARINE/OFFSHORE  
ASSET TYPES

FOR VARIOUS OWNERS

- NAVIGATION
- CONTROL SYSTEMS
- SURVEILLANCE SYSTEMS



---

# ABS CyberSafety<sup>®</sup> Approach

- Establish a staffed cybersecurity program for Industrial Control Systems (ICS)
- Develop an incident response capability
- Implement a Cybersecurity Management System
- Establish a formal management of change system
- Develop formal ICS cybersecurity training




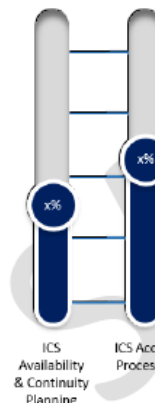


---

# ABS CyberSafety Engagement Options

- Policies and Procedures review
  - Incident response team members & associated responsibilities
  - Software Management of Change policy
  - Description of cybersecurity training policy and procedures
- Formal Vessel Assessment
  - Pre-Assessment Phase including data collection and information sharing
  - Office and Vessel visit applying 200+ point criteria
  - Formal report including findings, recommendation & CS1 gap analysis
- ABS CyberSafety Notation
  - Verification of policies & procedures, Cybersecurity Management System, crew awareness, documentation, etc
  - Vessel visit...confirmation (or gap analysis) of a CSx notation
- Annual/Renewal Survey of CSx Notation
  - Verification during normal Survey window (2-3 hrs. of surveyor time)

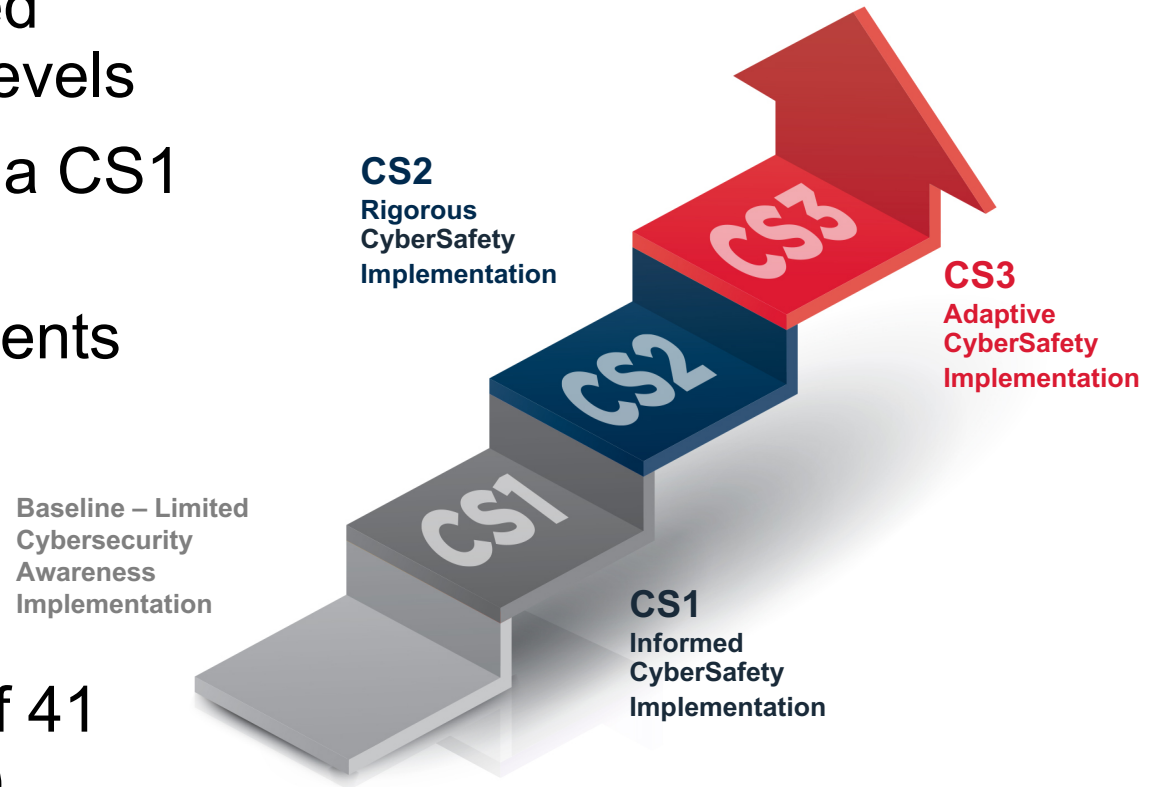
# ABS CyberSafety Assessment Reporting

 <p><b>ABS CyberSafety Assessment Technical Report of VESSEL for CLIENT</b></p> <p>Date: 2017</p> <p>SUBMITTED TO: CLIENT</p> <p>SUBMITTED BY: American Bureau of Shipping</p> <p><b>ABS</b></p>	<p><b>Table of Contents</b></p> <ol style="list-style-type: none"> <li>1 Executive Summary</li> <li>2 Introduction</li> <li>3 Summary</li> <li>4 Documentation</li> <li>5 On-Assessment</li> <li>6 Remediation</li> <li>7 Conclusion</li> <li>8 Appendix A – Conformance</li> <li>9 Appendix B – Reviewed Data</li> </ol>  <p>ICS Availability &amp; Continuity Planning</p> <p>ICS Access Process</p>	<table border="1"> <thead> <tr> <th>ID #</th> <th>ABS CyberSafety Guide Specifications</th> <th>Assessment Discovery</th> <th>Path to Closure</th> <th>Note</th> </tr> </thead> <tbody> <tr> <td>2.4.5.</td> <td>Establish and document an incident response and continuity plan for each ICS function by incident level of severity an incident type. Include restoration and recovery activities, backup activities (e.g., frequency and safe storage), test activities, and communication plan. For additional information, also see the ICS MOC section in this policy. Submit the plan to the ICS Cybersecurity Office for approval.</td> <td>No indication of incident response plan developed by CLIENT.</td> <td>Provide a means for collecting data onboard the asset. Develop an incident response plan and procedure with risk analysis for a given ICS.</td> <td><b>Major discrepancy.</b></td> </tr> <tr> <td>2.4.6.</td> <td>Respond to each incident based type, severity, and the response protocol established by the approved incident response and continuity plan.</td> <td>No indication of incident response plan developed by CLIENT.</td> <td>Develop and implement an Incident Response Plan (or a Business Continuity Plan) with responsible personnel, incident rating, and a process to respond to an incident.</td> <td>Recommend determine answers to: <ul style="list-style-type: none"> <li>Who responds to ICS incidents within CLIENT?</li> <li>What is the process to respond?</li> <li>What is the approval process for incident response?</li> </ul> </td> </tr> <tr> <td>2.4.7.</td> <td>Document and report all ICS cybersecurity incidents by occurrence, severity, and type.</td> <td>No indication of incident response plan developed by CLIENT.</td> <td>Develop a process to collect and report ICS breaches, incidents, and any anomalous activities. Rank the incidents based on the severity.</td> <td>Risk analysis, FMECA, FMEA on the ICS that includes cybersecurity incidents.</td> </tr> </tbody> </table>	ID #	ABS CyberSafety Guide Specifications	Assessment Discovery	Path to Closure	Note	2.4.5.	Establish and document an incident response and continuity plan for each ICS function by incident level of severity an incident type. Include restoration and recovery activities, backup activities (e.g., frequency and safe storage), test activities, and communication plan. For additional information, also see the ICS MOC section in this policy. Submit the plan to the ICS Cybersecurity Office for approval.	No indication of incident response plan developed by CLIENT.	Provide a means for collecting data onboard the asset. Develop an incident response plan and procedure with risk analysis for a given ICS.	<b>Major discrepancy.</b>	2.4.6.	Respond to each incident based type, severity, and the response protocol established by the approved incident response and continuity plan.	No indication of incident response plan developed by CLIENT.	Develop and implement an Incident Response Plan (or a Business Continuity Plan) with responsible personnel, incident rating, and a process to respond to an incident.	Recommend determine answers to: <ul style="list-style-type: none"> <li>Who responds to ICS incidents within CLIENT?</li> <li>What is the process to respond?</li> <li>What is the approval process for incident response?</li> </ul>	2.4.7.	Document and report all ICS cybersecurity incidents by occurrence, severity, and type.	No indication of incident response plan developed by CLIENT.	Develop a process to collect and report ICS breaches, incidents, and any anomalous activities. Rank the incidents based on the severity.	Risk analysis, FMECA, FMEA on the ICS that includes cybersecurity incidents.
ID #	ABS CyberSafety Guide Specifications	Assessment Discovery	Path to Closure	Note																		
2.4.5.	Establish and document an incident response and continuity plan for each ICS function by incident level of severity an incident type. Include restoration and recovery activities, backup activities (e.g., frequency and safe storage), test activities, and communication plan. For additional information, also see the ICS MOC section in this policy. Submit the plan to the ICS Cybersecurity Office for approval.	No indication of incident response plan developed by CLIENT.	Provide a means for collecting data onboard the asset. Develop an incident response plan and procedure with risk analysis for a given ICS.	<b>Major discrepancy.</b>																		
2.4.6.	Respond to each incident based type, severity, and the response protocol established by the approved incident response and continuity plan.	No indication of incident response plan developed by CLIENT.	Develop and implement an Incident Response Plan (or a Business Continuity Plan) with responsible personnel, incident rating, and a process to respond to an incident.	Recommend determine answers to: <ul style="list-style-type: none"> <li>Who responds to ICS incidents within CLIENT?</li> <li>What is the process to respond?</li> <li>What is the approval process for incident response?</li> </ul>																		
2.4.7.	Document and report all ICS cybersecurity incidents by occurrence, severity, and type.	No indication of incident response plan developed by CLIENT.	Develop a process to collect and report ICS breaches, incidents, and any anomalous activities. Rank the incidents based on the severity.	Risk analysis, FMECA, FMEA on the ICS that includes cybersecurity incidents.																		

---

# ABS Cybersafety Notations

- Vessels are assessed against all notation levels
- Two vessels earned a CS1 notation
- Completed assessments show an average conformity level of 35% to CS1 requirements
- OK approx. 14 out of 41 Requirements (CS1)



ABS CyberSafety® Notations/Certificates

---

# Common Industry Challenges – Versus CS1 Notation

88%

Missing or inadequate Management of Change policies and procedures

63%

Missing or inadequate Incident Response Capability

63%

Vessel's crew lacked cyber hygiene awareness

50%

Lack of OT network activity monitoring

# .... success implementation of cyber protection

Driven from  
the top

Corporate  
Firewall is  
not enough

OT and IT

Procedures  
in place

Cyber Hygiene

Incident  
Response  
Plan

Continuous  
Improvement



© Igor Karasi/Shutterstock



---

# Some considerations...

- The goals are not smarter ships or digital operation per se, the goals are a safer and more efficient shipping industry and smarter ways to operate
- Assets get smarter, the future is data-centric and the management of data integrity is a key
- Cyber Safety and Cyber Security protection are fundamental
- An adequate Cyber Protection culture aims to build the human understanding of how this risk works

---

# Global Reach and Support

- Dedicated ABS CyberSafety team
- Recognized by industry and government
- ABS CyberSafety® Laboratory provides research and development to support a global team





---

**Thank You**

[www.eagle.org](http://www.eagle.org)







How to save money, time and stay in compliance with IT and comms.

Eric Jan Bakker

VP Sales Asia Pacific,  
Marlink

[marlink.com](http://marlink.com)



## Data centric & Connected technologies for shipping

Eric Jan Bakker, VP Sales Asia Pacific

# Data-centric & Connected ships

## Ship Efficiency

Become part of the ship operations; give shipping companies competitive advantages with integrated and standardized tools

## Security & Safety

Enhance security of vessel management (cyber), improve processes to be in line with maritime regulations & navigation standards

## Crew Wellbeing

Provide solutions for shipping companies to attract and retain good crew, with tools that do not impact the business critical applications

## Ship IT

Enable core services to facilitate communication services at sea and ease staff on shore to focus on their core activities remotely

## Solving Main Challenges

Fuel Reduction

Preventive Maintenance

eNavigation

Secured ICT

Crew Health

Compliance & Document handling

Crew Privat Comms

On board Education

Entertainment

Cyber security

Remote IT Mngt

Collaboration Tools

Whitepaper:



# The Maritime Industry at the Dawn of Digitalisation



Connected & Smart Ships: Hype or Reality?  
Download our free whitepaper

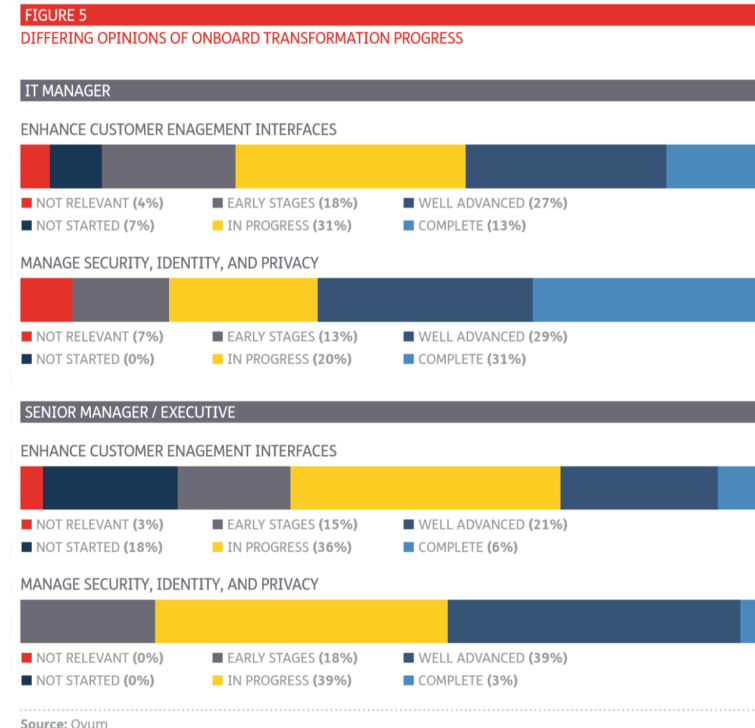


Register on [www.marlink.com](http://www.marlink.com)

# The Maritime Industry at the Dawn of Digitalisation



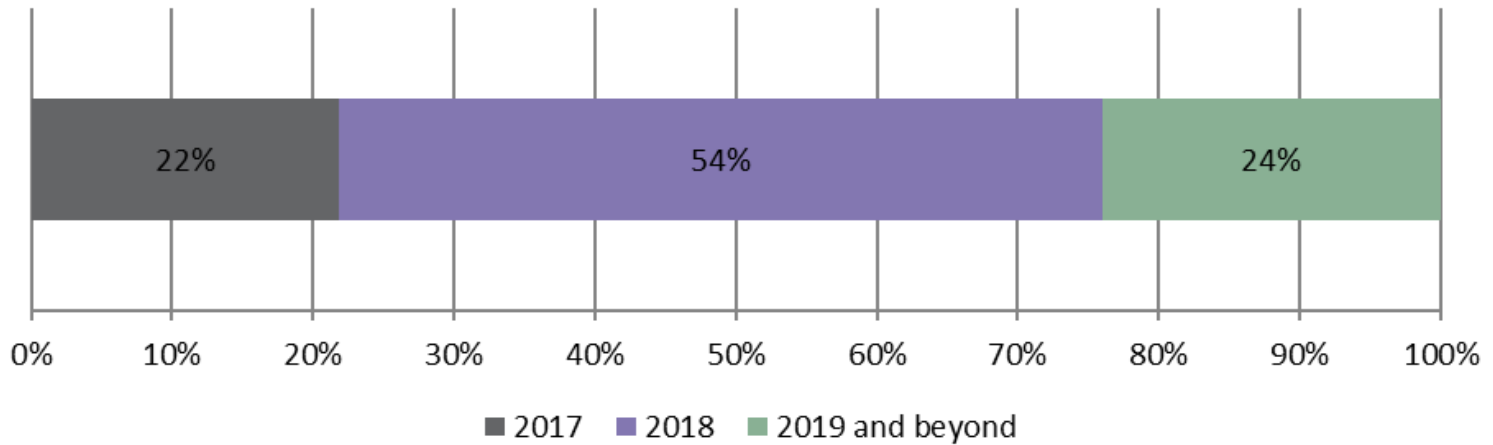
- THE MARITIME INDUSTRY IS “DIGITAL READY”
  - 2/3<sup>rd</sup> have standardized satellite communications & IT solutions
  - 81% of the companies have >5 staff in ICT
  - only 30% are “well advanced” or “in progress”
- VSAT implementation initiated in 2/3<sup>rd</sup> of companies.
- Market Drivers
  - low earnings & weak financials
    - increasing operating efficiency
    - reducing operating expenditures
    - improving **customer experience**
- Achieved so far
  - navigation/ ECDIS
  - on-board wireless networks
  - standardized vessel IT-infrastructure & software and maintenance
  - remote management solutions



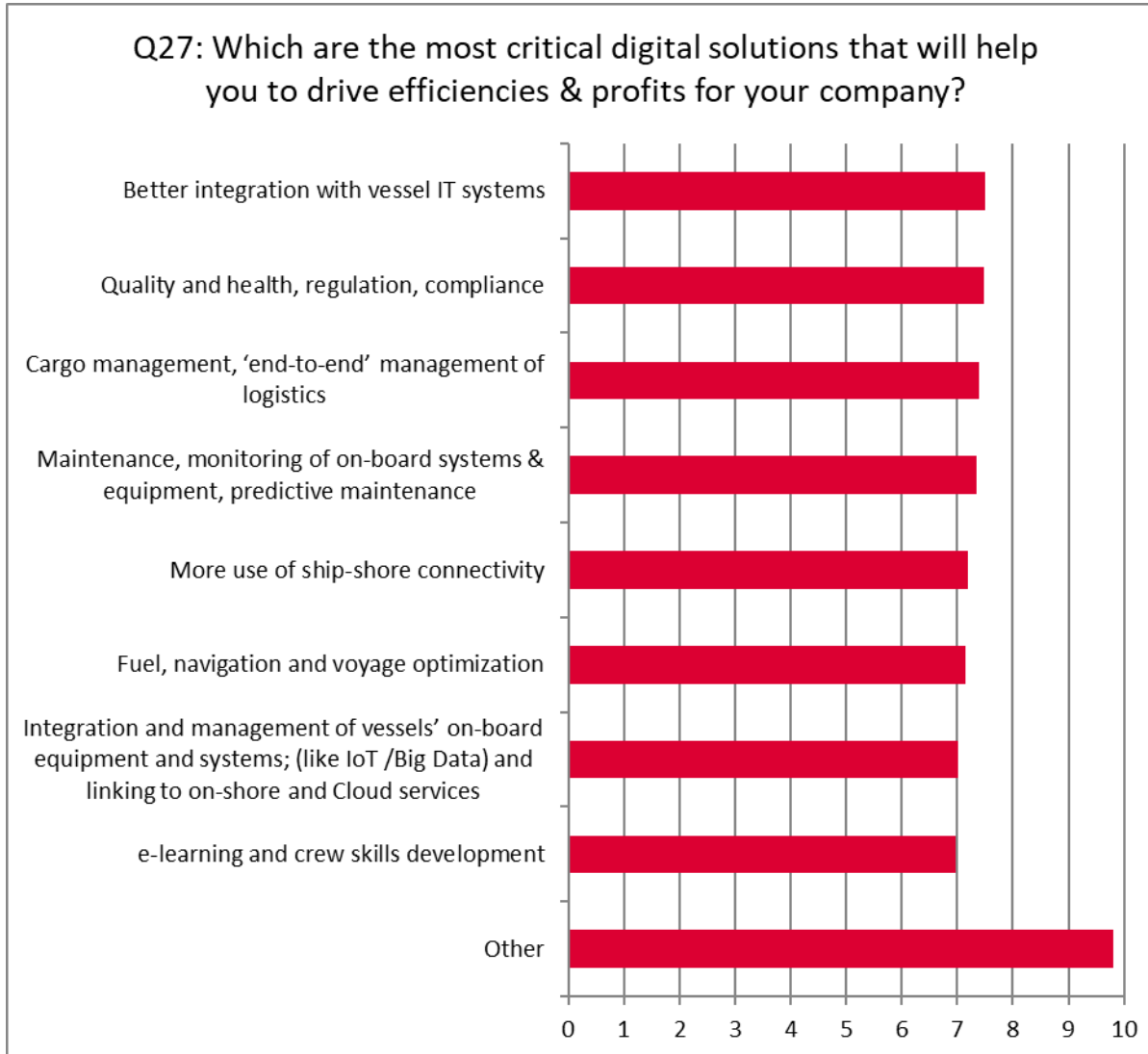
# Investment time frames



Q30a For those firms that intend to deploy the listed digital solution areas, when do you expect these plans to be carried out?



# Digital solutions are designed to help drive efficiencies and profit

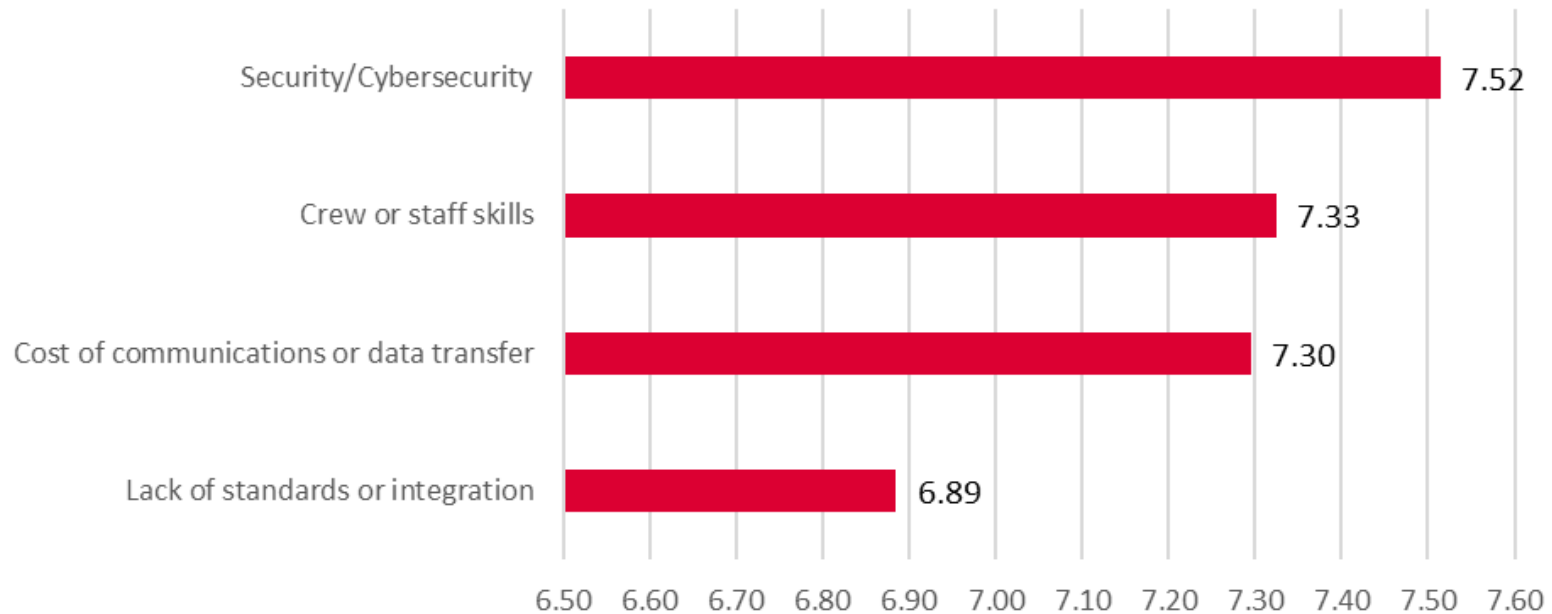




# Four barriers to adopting digitalisation



Q31: How significant are the following potential barriers in adopting digitalization?



Whitepaper:



# The Maritime Industry at the Dawn of Digitalisation



Connected & Smart Ships: Hype or Reality?  
[Download our free whitepaper](#)



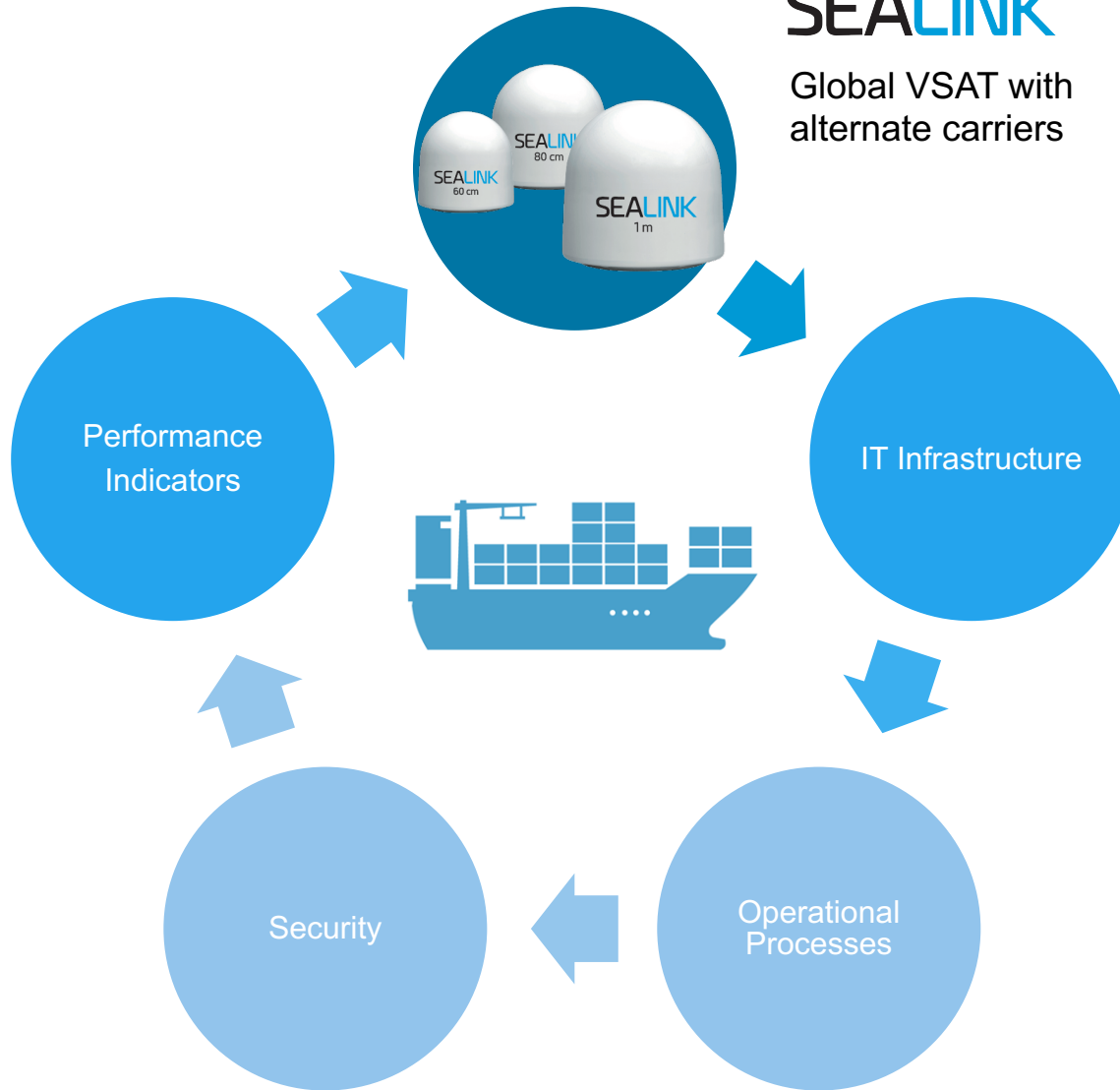
Register on [www.marlink.com](http://www.marlink.com)

# Integrated Digital Approach

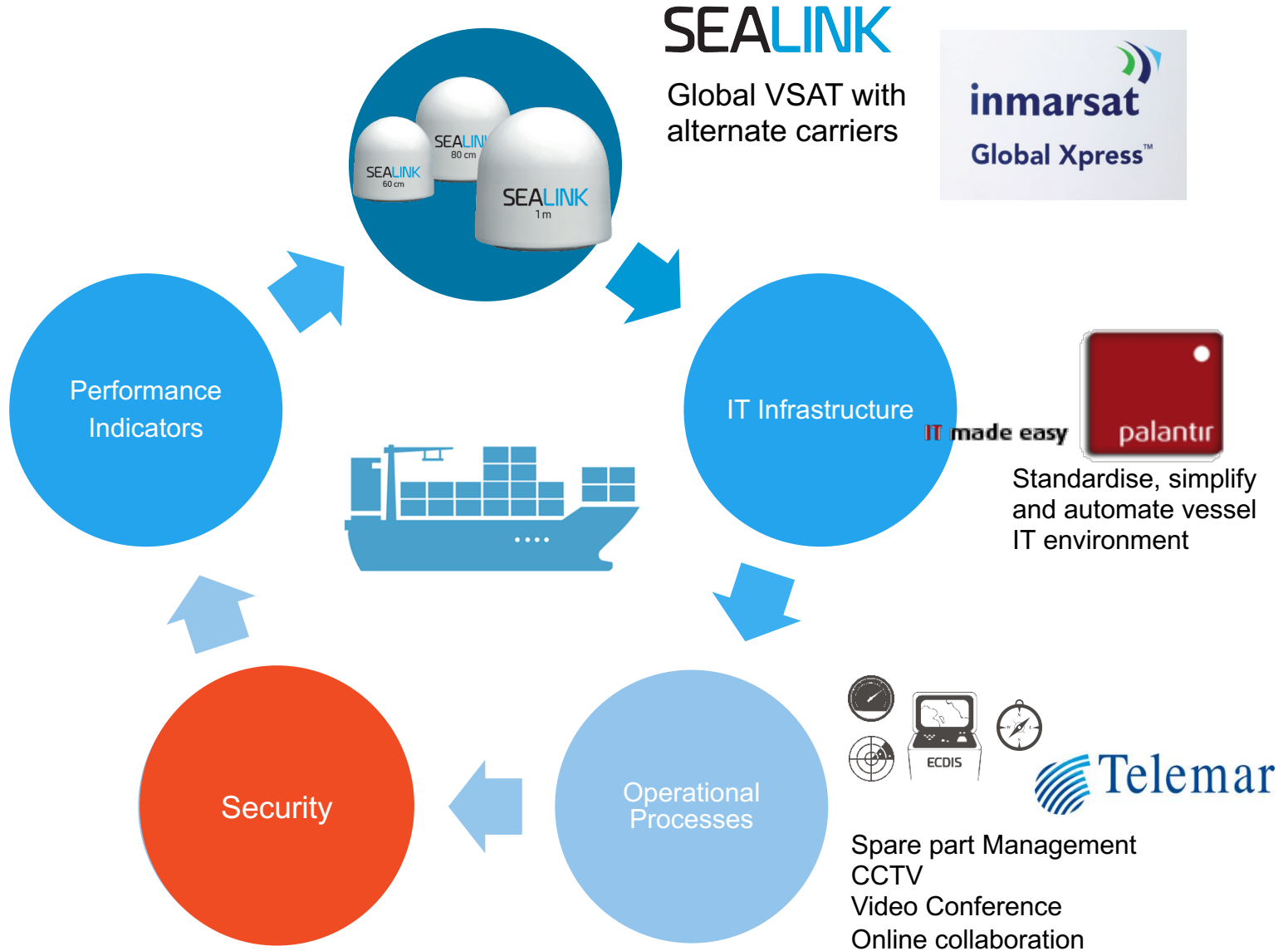


**SEALINK**

Global VSAT with  
alternate carriers



# Integrated Digital Approach



# With Digitalisation Comes Security



## WannaCry' ransomware attacks

Wide attack has crippled more than 300,000 computers in 150 countries

Information of computers attacked by the 'WannaCry' ransomware\*

Recorded by security blog MalwareTech in the 24 hours up to May 16, 00:00GMT

## SPLASH24/7

RIGHTSHIP Qi

HOME SECTOR REGION MARITIME CEO CONTRIBUTIONS OPINION MAGAZINES SPLASH TV JOB

Home / Sector / Containers

## Maersk makes contingencies in the wake of Petya ransomware attack

JUNE 29TH, 2017 SAM CHAMBERS

CONTAINERS, EUROPE, PORTS AND LOGISTICS, TECH 0 COMMENTS

As of Wednesday evening Maersk Line said it was taking bookings via box platform INTTRA in the wake of Tuesday's cyber attack while sister firm APM Terminals said most of its terminals were back up operating, albeit not all of them at normal speeds.

The Maersk Group became the most high profile maritime hacker victim in history on

## SHIP TRACKER

TOTAL: 87777

### NEWSLETTER

Sign Up Now

### SPLASH DASH

Editor's Picks

#### Top Ships faces legal action over its Kalani dealings

Another Greek owner with links to controversial Kalani Investments has seen lawyers gear up for a...

AUG 25TH, 2017 IN | TANKERS

#### China's letter of serious intent

The letter of intent signed between state-backed CSSC and France's CMA CGM for record-breaking...

AUG 25TH, 2017 IN | SHIPYARDS

Home / Region / Europe

## Ship's satellite communication system hacked with ease

JULY 19TH, 2017 SAM CHAMBERS EUROPE, OPERATIONS, TECH 2 COMMENTS

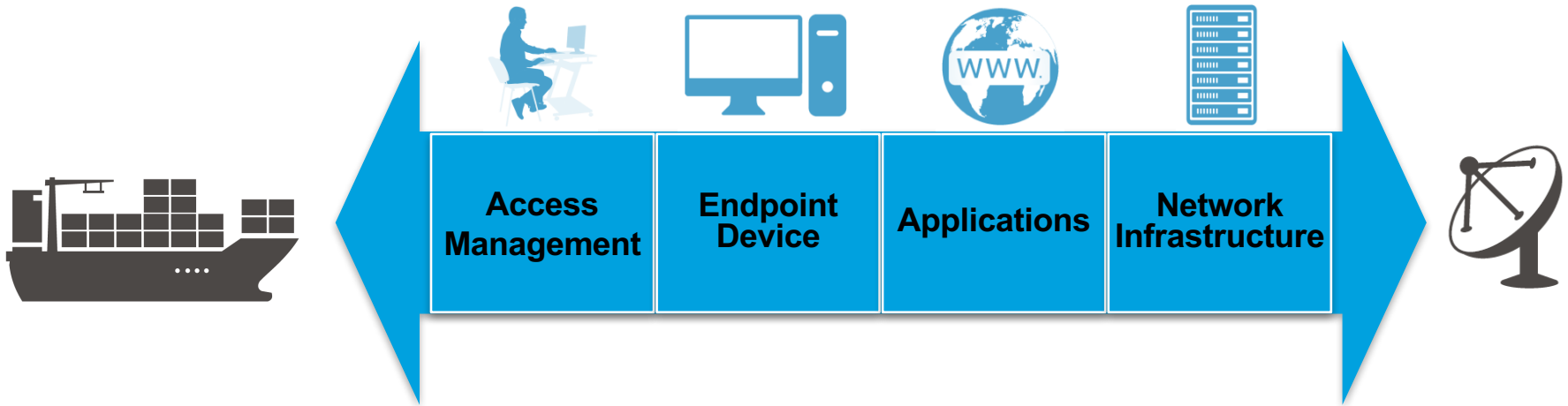
The vulnerability of shipboard systems has been laid bare for all to see on social media.

Splash has seen how one France-based security researcher was able to enter the satellite communications system of a ship in mid-voyage by entering simple username and passwords. The researcher used the search engine Shodan to find easy online targets at sea.

# Marlink's Security Portfolio



## Multi-Layered Security Solutions



# Integrated Digital Approach



## SEALINK

Global VSAT with alternate carriers



Performance Indicators

IT Infrastructure

IT made easy

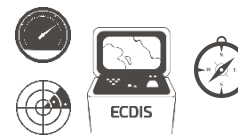


Standardise, simplify and automate vessel IT environment



Security

Operational Processes



Spare part Management  
 CCTV  
 Video Conference  
 Online collaboration

Marlink's Security Portfolio

Multi-Layered Security Solutions

Access Management | Endpoint Device | Applications | Network Infrastructure

X-CHANGE

SKYFILE ANTI VIRUS | KeepUp@Sea | SEALINK

PORTAL360

Data centric & connected technologies



**Enable evidence based decision making**

**Drive the Digital Fleet, rather than the Digital Ship**

**Create a platform for collaboration**

**Within the maritime industry**



Data centric & connected technologies



**Enable evidence based decision making**

**Drive the Digital Fleet, rather than the Digital Ship**

**Create a platform for collaboration**

**With your customers**

Data centric & connected technologies



**Enable evidence based decision making**

**Drive the Digital Fleet, rather than the Digital Ship**

**Create a platform for collaboration**

**Within your organization**

Data centric & connected technologies



**Enable evidence based decision making**

**Drive the Digital Fleet, rather than the Digital Ship**

**Create a platform for collaboration**

**With your partners and suppliers**

# Data centric & connected technologies



**Enable evidence based decision making**

**Drive the Digital Fleet, rather than the Digital Ship**

**Create a platform for collaboration**

**Compliance**



**New Technologies**



**Cyber Security**





Time for  
interaction & collaboration

[Ericjan.Bakker@Marlink.com](mailto:Ericjan.Bakker@Marlink.com)

# Time for interaction





Connect smarter. Anywhere.

# Contributors



The Norwegian Chamber of Commerce in Hong Kong (NCC) was established in 1984 and is a forum for representatives of Norwegian companies in Hong Kong, representatives of local companies which have links to Norway or take an interest in Norway, as well as individuals. Chamber objectives:

- To arrange for the exchange of information and experience between members of The Chamber
- To make suitable representations on behalf of the Norwegian business community in Hong Kong to the competent authorities and institutions in Hong Kong and Norway
- To promote commercial exchange between Norway and Hong Kong
- To contribute to the enhancement of the image of Norway in Hong Kong; and
- To promote knowledge of Hong Kong within Norwegian business.

[ncchk.org.hk](http://ncchk.org.hk)



Palantir AS, founded year 2000, is a Norwegian registered ISO9001 certified IT & communication company. Headquarter is located in Norway (Stord), with subsidiaries in Singapore, Manila and Copenhagen.

Through their KeepUp@Sea solution Palantir enables shipowners and operators to improve efficiency of vessel IT-operations, at the same time as the solution helps customers to protect against enhanced cyber security threat.

Palantir's vision is to go on board the vessel once during a hardware lifecycle, thereafter the entire fleet-IT solution is managed and automatically monitored from shore side. For their partners this means increased uptime, fewer support tickets, and less need to board vessels due to IT issues. Over 1000 vessels are signed up with Palantir's KeepUp@Sea solution.

Palantir AS have since last three years enjoyed a close partnership with Marlink, and in March 2017 Marlink acquired 100% of Palantir AS' shares. As a global organisation they will together continue to offer diverse service added value, providing maritime businesses with seamless IT, communications and electronics solutions.

[palantir.no](http://palantir.no)



Seagull Maritime AS is the leading provider of competence management solutions and e-learning material for seafarers worldwide and offers a comprehensive library of training and onboard courses for regulatory compliance and improved seafarer knowledge.

Founded in 1996 by experienced mariners we have grown into a dynamic company in partnership with leading shipping companies to deliver a full range of competence management, training administration, assessment and training tools that ensure meeting and exceeding STCW and IMO standards.

[seagull.no](http://seagull.no)



NAVTOR is a leading force in the provision of innovative e-Navigation solutions, and a total supplier of navigational products and services for the maritime sector. Every day we strive to make life easier for navigators, and safer, clearer and more efficient for shipowners, ship managers and operators.

The headquarter of NAVTOR is in Egersund, Norway, and the subsidiaries are located in Singapore (NAVTOR Singapore Ltd. Ptd.), Japan (NAVTOR Japan K.K.) Sweden (NAVTOR NAUTIC AB) The United Kingdom (NAVTOR UK Ltd.), The United States of America (NAVTOR USA Inc.) and Russia (NAVTOR Russia LLC).

[navtor.com](http://navtor.com)



