Transport DTU
Centre for Transport Research

DTU

Cyber Resilience for the Shipping industry (CyberShip)

Michael Bruhn Barfod, Associate professor, project leader

Background: The shipping industry has become more vulnerable to cyber-attacks in recent years, because of its dependence on information technology and increasingly complex networks. Cyber systems are incorporated into almost every facet of maritime operations (GNSS, AIS, ECDIS etc.). All maritime structures (including ships and offshore facilities) as well as the connected infrastructure are vulnerable. Currently, the awareness regarding cyber security aspects at ships either is at a very low level or completely disregarded.

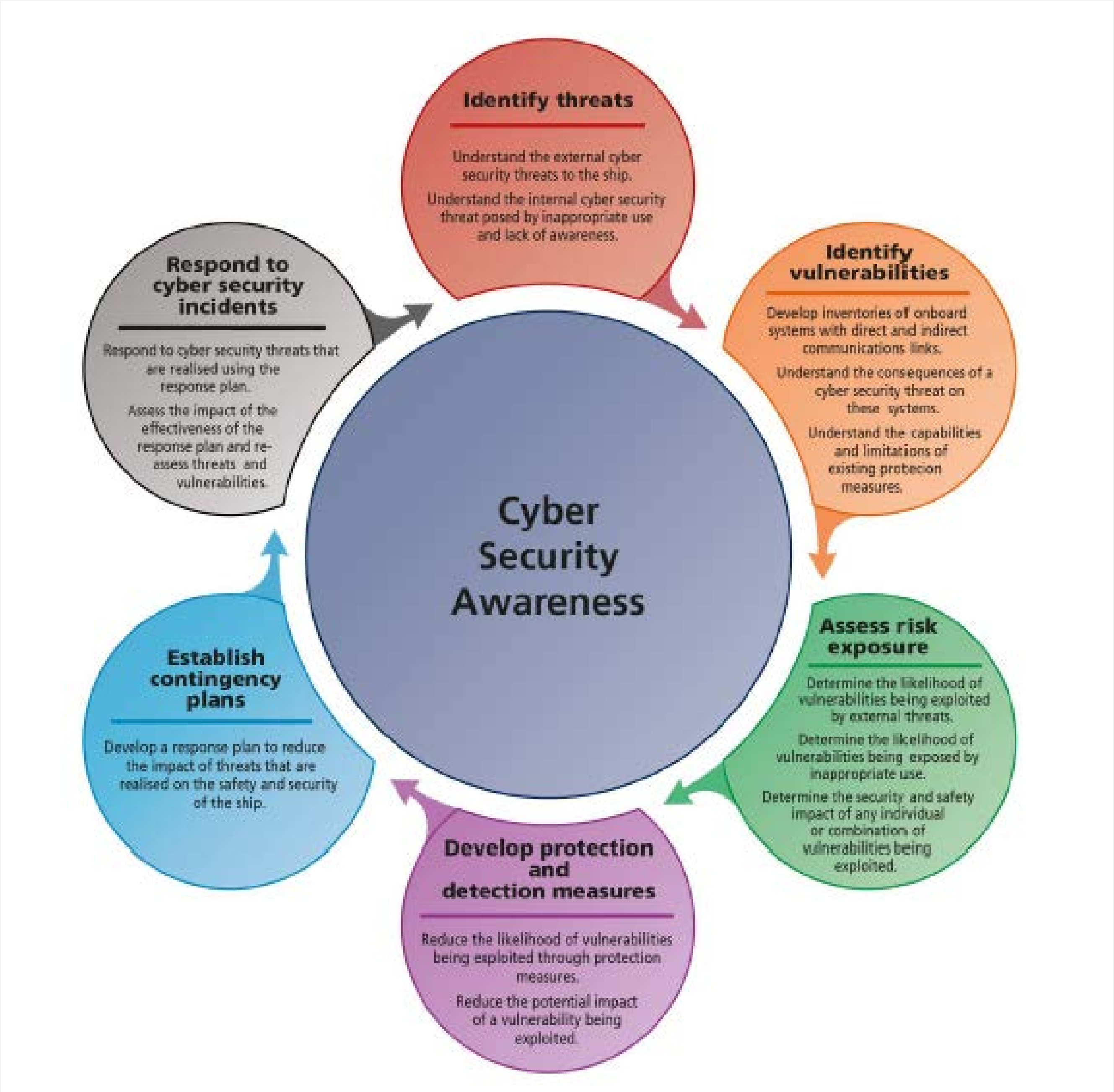

Identify threats
Understand the external cyber security threats to the ship.
Understand the internal cyber security threat posed by inappropriate use and lack of awareness.
Identify vulnerabilities
Develop inventories of onboard systems with direct and indirect communications links.
Understand the consequences of a cyber security threat on these systems.
Understand the capabilities and limitations of existing protecion measures.
Assess risk exposure
Determine the likelihood of vulnerabilities being exploited by external threats.
Determine the likelihood of vulnerabilities being exposed by inappropriate use.
Determine the security and safety impact of any individual or combination of vulnerabilities being exploited.
Develop protection and detection measures
Reduce the likelihood of vulnerabilities being exploited through protection measures.
Reduce the potential impact of a vulnerability being exploited.
Establish contingency plans
Develop a response plan to reduce the impact of threats that are realised on the safety and security of the ship.
Respond to cyber security incidents
Respond to cyber security threats that are realised using the response plan.
Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.
Cyber Security Awareness

Figure 1: Cyber security awareness as set out in the guidelines by BIMCO (2016).

Guidelines:

To support the decision making process a set of tools will be developed for the assessment of identified key performance indicators (KPIs). Finally, a set of recommendations will be produced to direct the development of shipping cyber resilience in organizations via theoretically sound approaches such as scenario planning and real options. The baseline of the project will be the current BIMCO guidelines on this subject.

Key players from the industry be included in the Advisory Committee of the project.

Purpose:

The aim of CyberShip is to propose a framework for improving the resilience of the shipping industry to cyber risks, with the ship being its main focus.
The novel theoretical framework will combine traditional risk management with systems analysis and control theory to aid the decision making process of shipping companies in the detection, identification, and prevention of cyber-attacks, as well as guide the recovery and response process and organizational adjustment (learning process) following a cyber-attack.

A strong emphasis through CyberShip is put on bridging the gap between traditional risk management and IT Management, rendering an operational framework model possible for implementation within the shipping industry. The framework model will consider both systems analysis, to identify the network characteristics, which allow it to react to disruptions, derived from cyber-attacks, and traditional risk management approaches.

The output of CyberShip will thus be an operational framework model that can be applied directly in the industry with the purpose of reducing the risk of cyber-attacks on ships. The framework model will be based on the newest research and will be state-of-the-art within the shipping area.

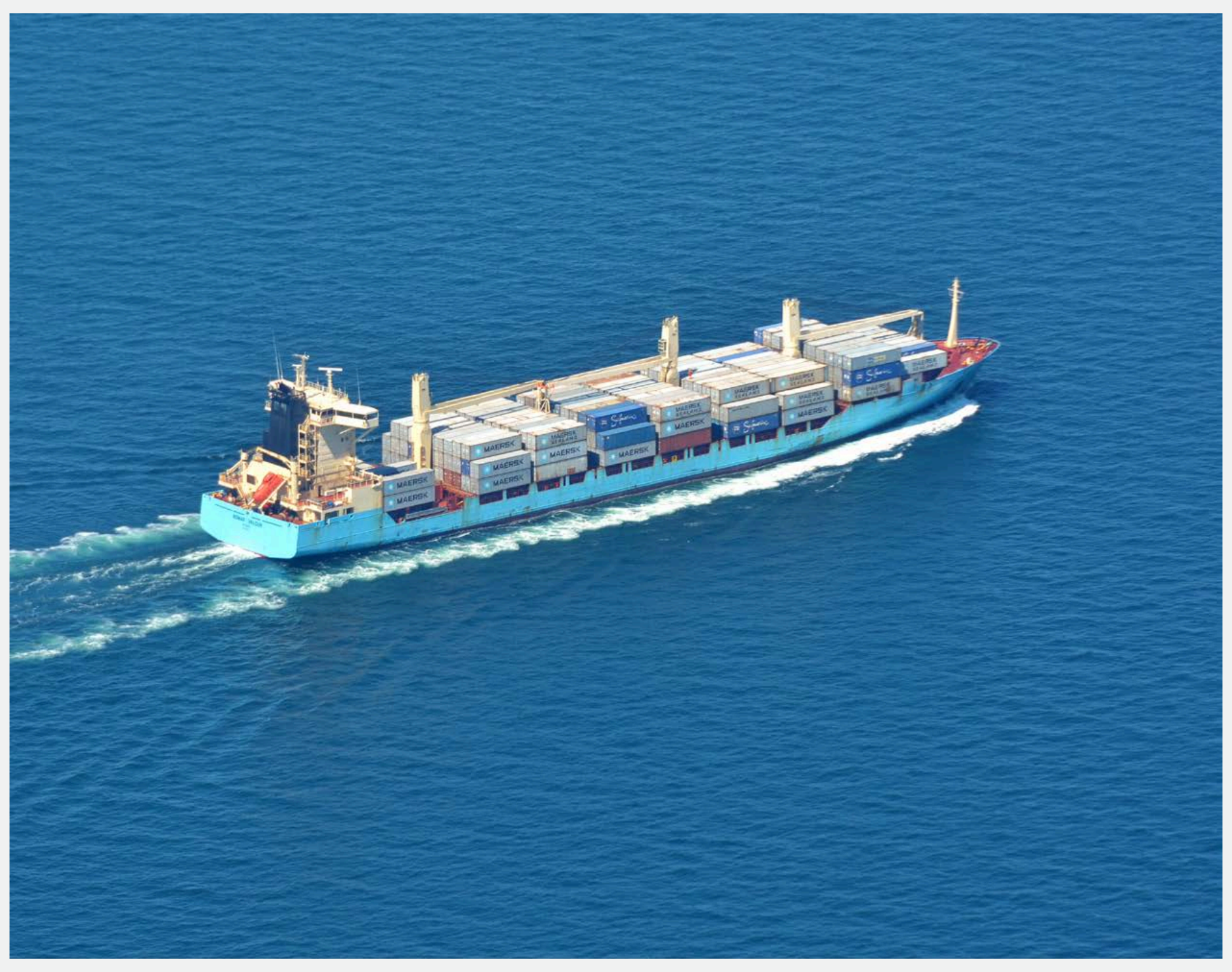
Project details:

Start date: September 1st 2017
End date: August 31st 2019

CyberShip is a joint project between DTU Management Engineering and DTU Compute.

The project will employ two post docs in the project period.

The project is funded by the Danish Maritime Fund and Orients Fund.



DTU Compute
Department of Applied Mathematics and Computer Science

DTU Management Engineering
Department of Management Engineering