IMO 2021 – striving towards a balanced approach

Jakob P. Larsen, Head of Maritime Safety & Security

jpl@bimco.org

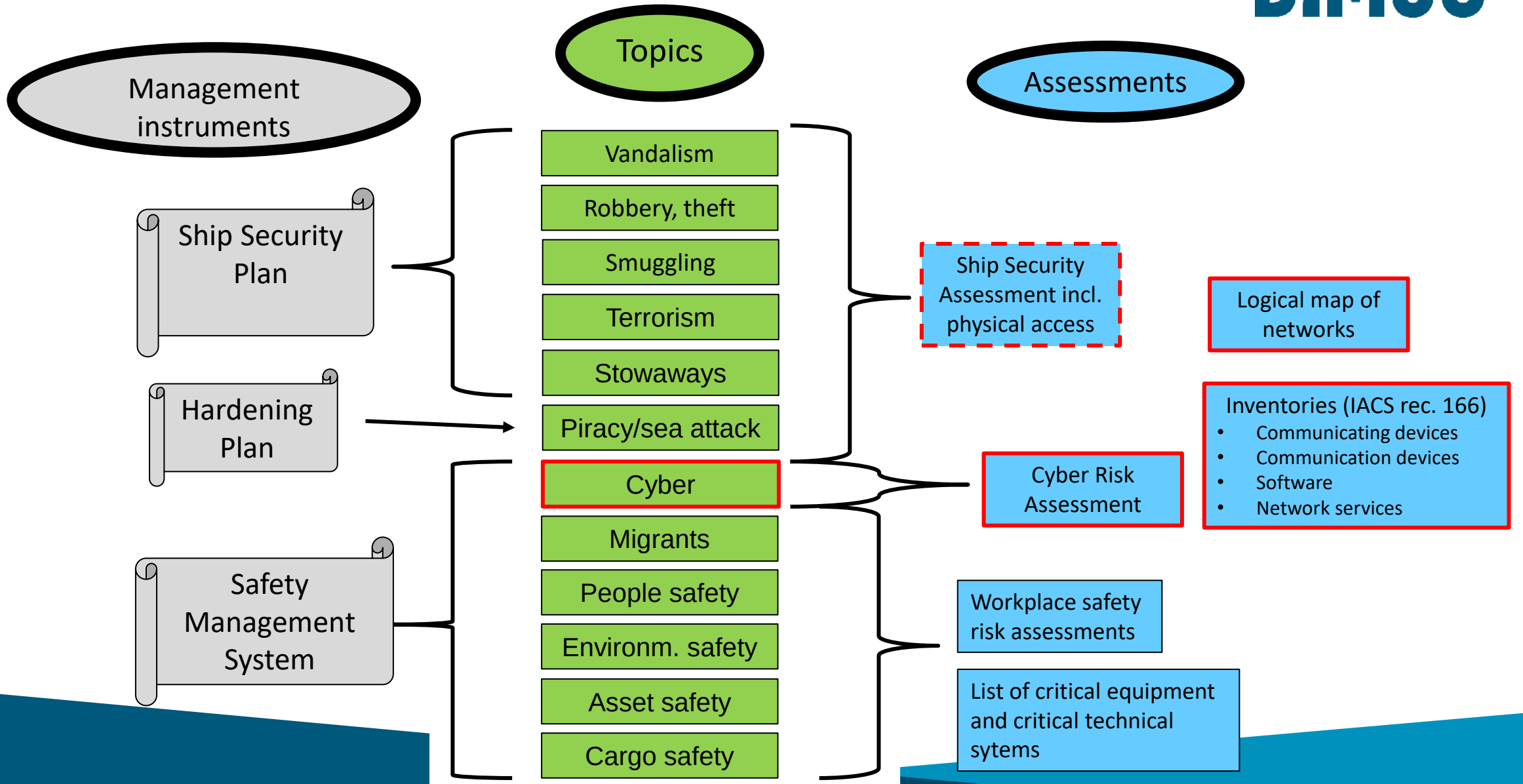
6th Ship IT conference, 28 September 2020

Copenhagen, 27 June 2017

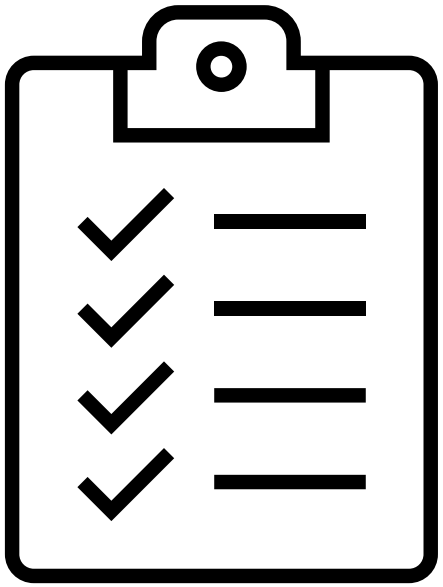
IMO resolution MSC.428(98) Maritime cyber risk management in safety management systems

- An approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code
- Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021
- precautions […] could be needed to preserve the confidentiality of certain aspects of cyber risk management

Managing cyber risks: a practical example



Risk assessment



ISM Code 1.2.2

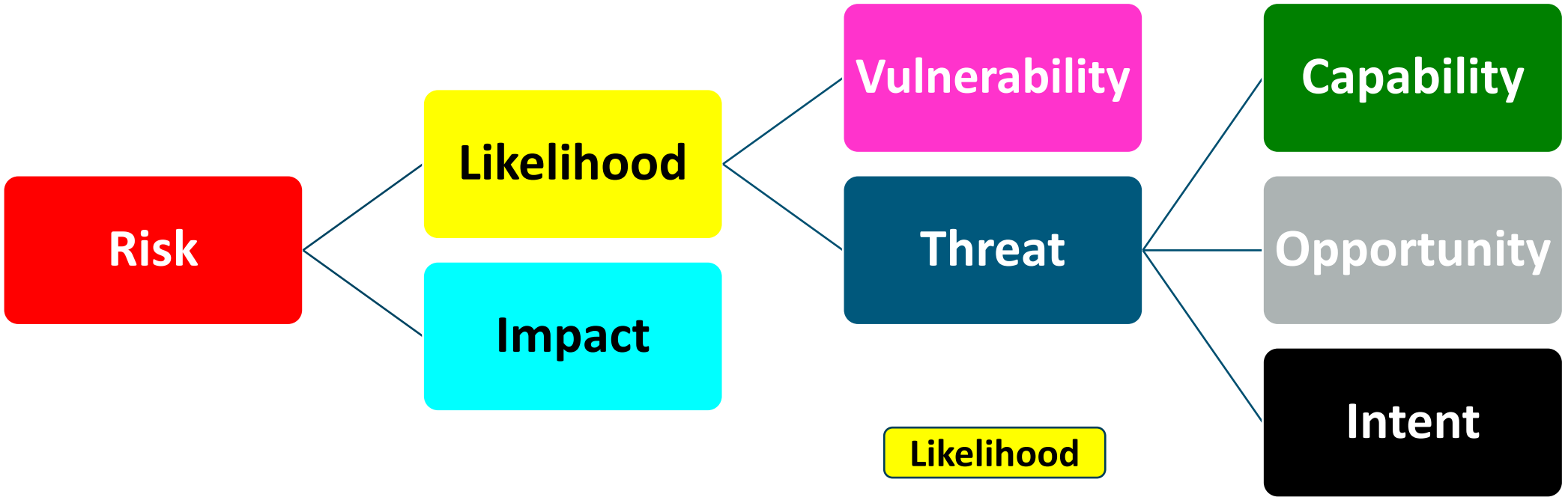
“Safety management objectives of the company should, inter alia:

1. […]
2. assess all identified risks to its ships, personnel and the environment and establish appropriate safeguards”

Industry guidance for cyber security on board ships

- Cyber security and safety management
- Threat identification
- Vulnerability identification
- Risk assessment
- Protection and detection measures
- Contingency plans
- How to respond and recover

Looking closer at risk as a concept

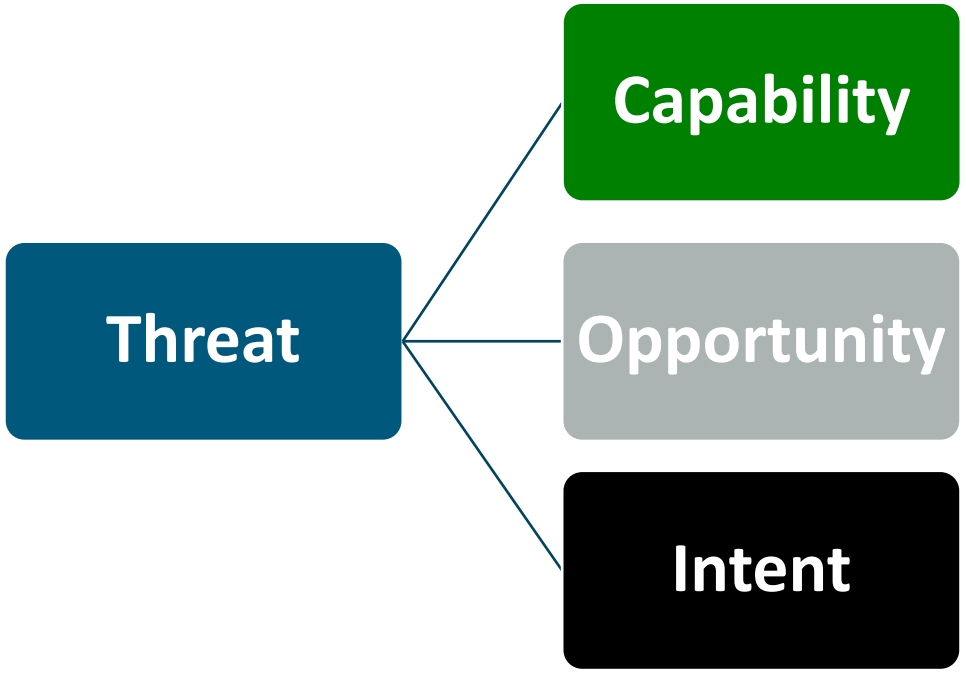


Likelihood

Risk = Impact x Vulnerability x (Capability x Opportunity x Intent)

Threat

Evaluating threats



Examples:

- Phishing
- Malware
- Hacking
- Social engineering
- Denial of service

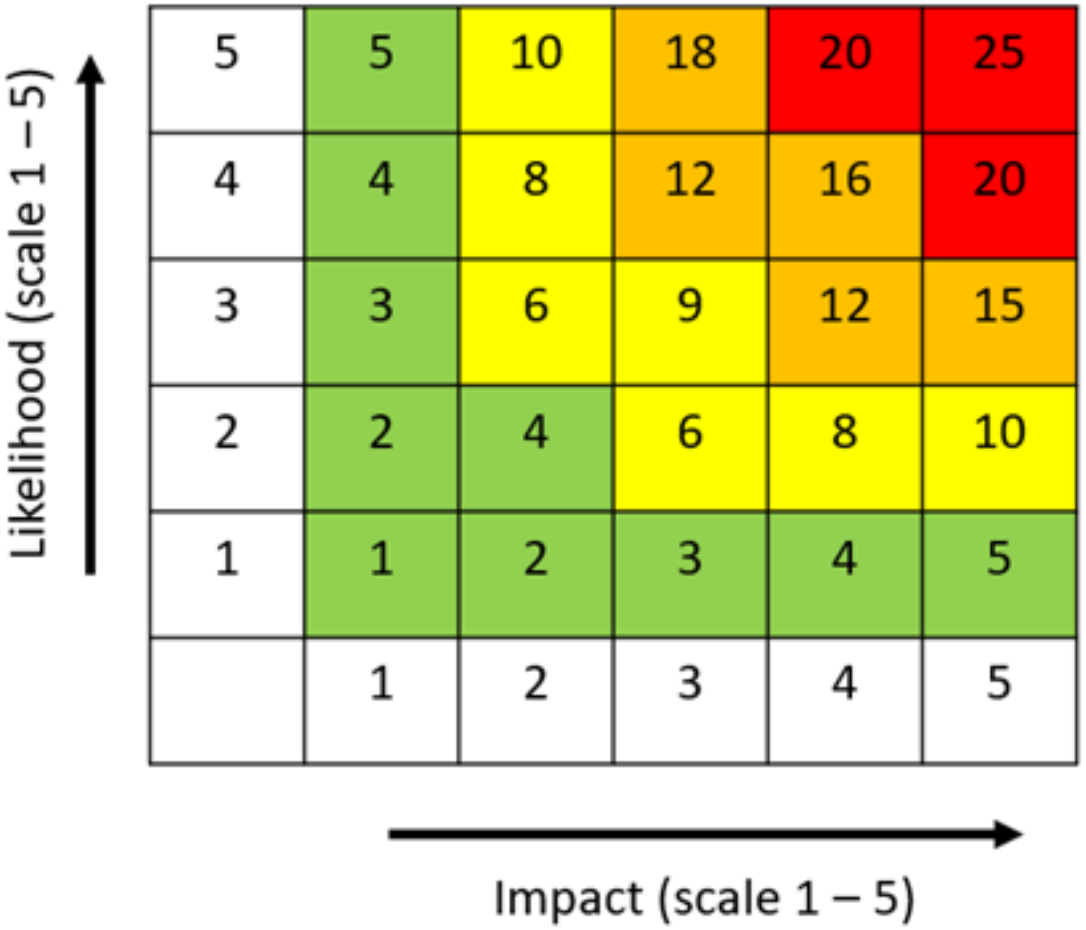
- Internet
- Wifi
- Removable devices
- Physical access

- Financial gain
- Vandalism
- Personal motives
- Political motives

Applicable to

- OT systems
- IT systems

Risk matrix

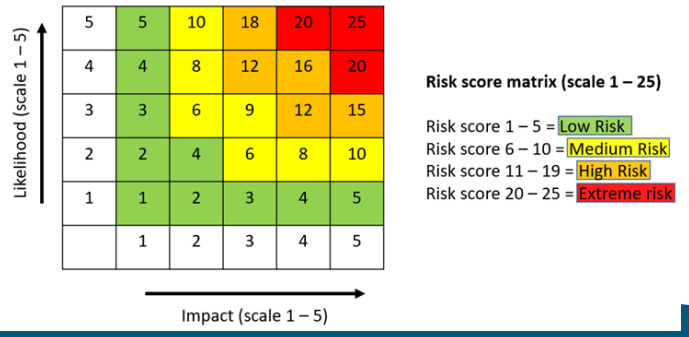


Risk score matrix (scale 1 – 25)

Risk score 1 – 5 = Low Risk
Risk score 6 – 10 = Medium Risk
Risk score 11 – 19 = High Risk
Risk score 20 – 25 = Extreme risk

Using existing SMS methodology

System	Impact	Likelihood	Initial Risk	Mitigation	Residual risk
ECDIS	Score 5 due to risk of catastrophic events like grounding and collision	Score 4 due to active USB ports, computer used for other purposes, connection to admin network for access to shared printer, connection to automatic chart updates via satellite via trusted vendor	Risk = 5 x 4 = 20	Password protect and restrict PC use to ECDIS only	Risk = 5 x 3 = 15
				Disconnect from admin network	Risk = 5 x 2 = 10
				Blind off USB ports	Risk = 5 x 1 = 5



Immediate steps

- Map remote accesses and data flows
- Segregate networks: critical systems, admin, crew, passenger
- Protect access to shipboard computers and systems (firewall, password management, removable media ports, physical access control)
- Protect email and other internet facing systems and software (antivirus)
- Initiate awareness training of all staff


Thank you
www.bimco.org