CYBEROWL

ReCAAP
Maritime cyber security

14th December 2021

Visibility | Security | Compliance

Agenda

1. Introduction
2. Cyber Security regulation for shipping
   - Catalyst for regulation
   - The regulation and it’s scope
   - How the regulation is interpreted
3. Cyber Security one year later
   - Overview of common risks and incidents
   - Driving forces for further improvement
4. Cyber Security and piracy
   - Similarities and differences
   - Convergence risk and mitigations
5. Conclusions

Introduction to CyberOwl

A team of data and security experts

Dan Ng

Chief Executive Officer

Russell Kempley

Chief Security Officer

Ken Woghiren

Chief Technical Officer

Professor Siraj Shaikh

Chief Science Officer

Award-winning Medulla technology

SAFETY4SEA
2021 Cyber Security Finalist

GCHQ

National Cyber Security Centre
a part of GCHQ

finalist
Cyber Security Awards

LLOYD'S
SCIENCE OF RISK PRIZE

FORRESTER®
NEW TECH: ICS SECURITY SOLUTIONS, Q1 2019
16 PROVIDERS "TO WATCH"

Deployed around the world

Cyber Security Regulation for Shipping

CYBEROWL

Why did marine cybersecurity need regulation?

Typical situation onboard vessels:

- Legacy Equipment
- Little or no patching
- Crew have full admin rights
- OEMs have little engagement
- Heavy use of removable media

Defence relies on limited connectivity

Trend towards digitalisation:

- More integration
- Greater dependence on automation
- More crew personal devices
- Remote maintenance
- Faster satellite links

Greater exposure and risk

Set against increasing threat landscape

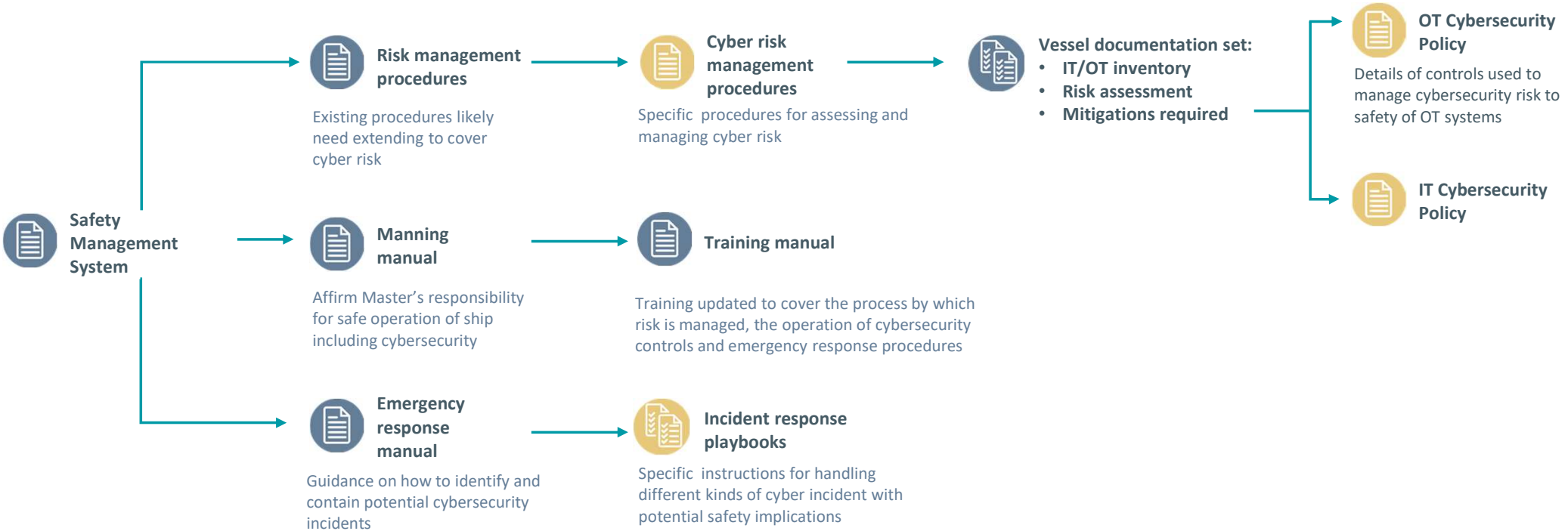
The regulation: IMO 2021

MSC.428(98):

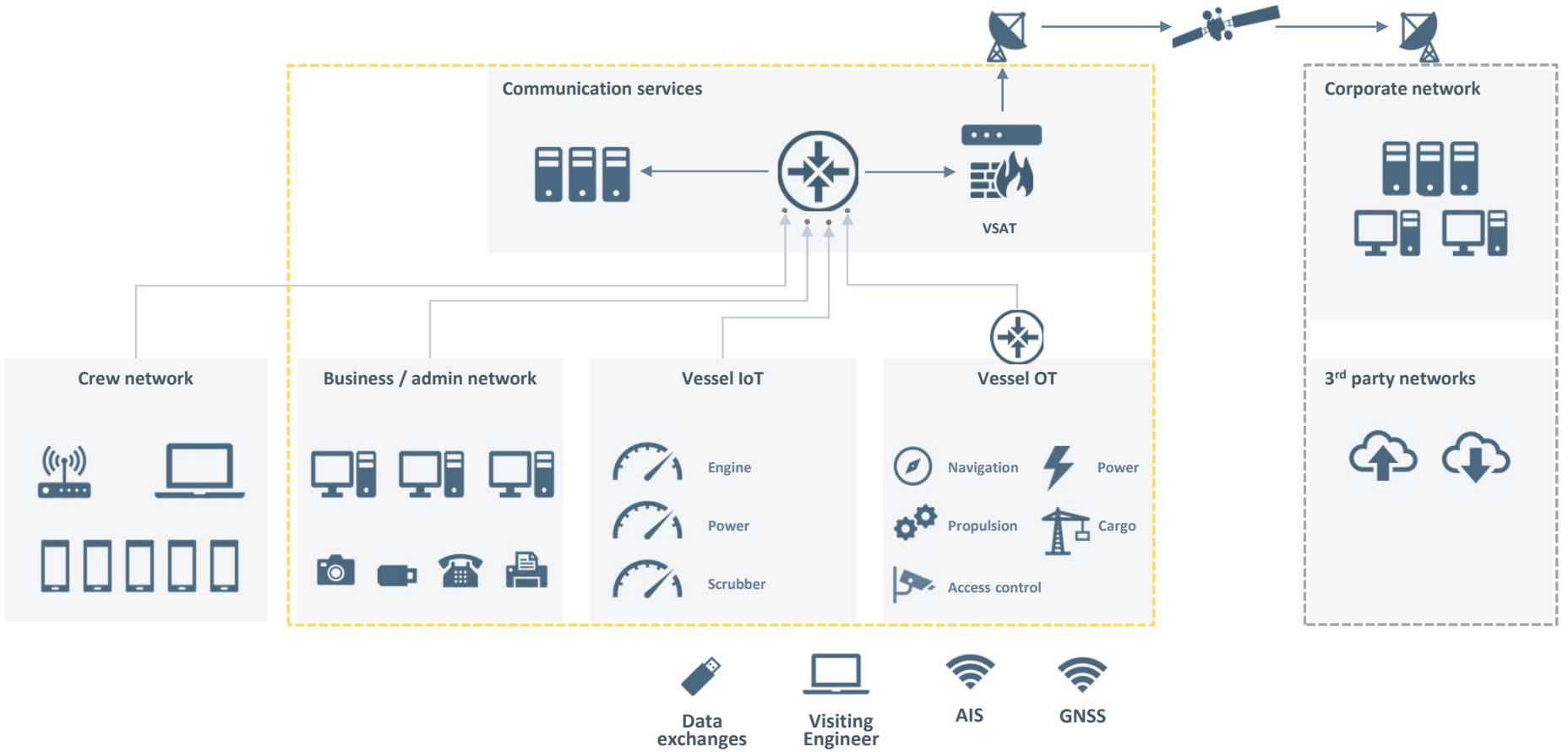
AFFIRMS that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code;

ENCOURAGES 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;

Safety Management System (SMS)



Scope of the ISM / SMS



Typical OT systems onboard

Communication systems

- integrated communication systems
- satellite communication equipment
- Voice Over Internet Protocols (VOIP) equipment
- wireless networks (WLANs)
- public address and general alarm systems
- systems used for reporting mandatory information to public authorities.

Bridge systems

- integrated navigation system
- positioning systems (GPS, etc)
- Electronic Chart Display Information System (ECDIS)
- Dynamic Positioning (DP) systems
- systems that interface with electronic navigation systems and propulsion/manoeuvring systems
- Automatic Identification System (AIS)
- Global Maritime Distress and Safety System (GMDSS)
- radar equipment
- Voyage Data Recorders (VDRs)
- Bridge Navigational Watch Alarm System (BNWAS)
- Shipboard Security Alarm Systems (SSAS).

Propulsion, machinery management and power control systems

- engine governor
- power management
- integrated control system
- alarm system
- bilge water control system
- water treatment system
- emissions monitoring
- heating, ventilation and air-conditioning monitoring
- damage control systems
- other monitoring and data collection systems eg fire alarms.

Cargo management systems

- Cargo Control Room (CCR) and its equipment
- onboard loading computers and computers used for exchange of loading information and load plan updates with the marine terminal and stevedoring company
- remote cargo and container tracking and sensing systems
- level indication system
- valve remote control system
- ballast water systems
- reefer monitoring systems
- water ingress alarm system.

Passenger or visitor servicing and management systems

- Property Management System (PMS)
- shipmanagement systems (often including electronic health records)
- financial related systems
- ship passenger/visitor/seafarer boarding access systems
- infrastructure support systems like domain naming system (DNS) and user authentication/ authorisation systems.
- incident management systems.

Passenger-facing networks

- passenger Wi-Fi or Local Area Network (LAN) internet access, for example where onboard personnel can connect their own devices[22]
- guest entertainment systems.

Core infrastructure systems

- security gateways
- routers
- switches
- firewalls
- Virtual Private Network(s) (VPN)
- Virtual LAN(s) (VLAN)
- intrusion prevention systems
- security event logging systems.

List of OT systems listed in BIMCO guidelines

Interpretation for guidance and audit

Regulation

International Maritime Organisation

MSC.428(98)

Global Standards

NIST

Guidance

MSC-FAL.1/Circ.3

BIMCO

Guidelines on Cyber Security Onboard Ships (v4)

Industry Associations

DCSA – Mar 2020

OCIMF VIQ7 – Feb 2019

Class societies

Specification of cyber security class notations

Audit

Port State Control

USCG CVC-WI-027 – Nov 2020

Other MOUs – TBC

Document of Compliance

Inspection and award of class notations

BIMCO Guidelines on Cyber Security onboard ships

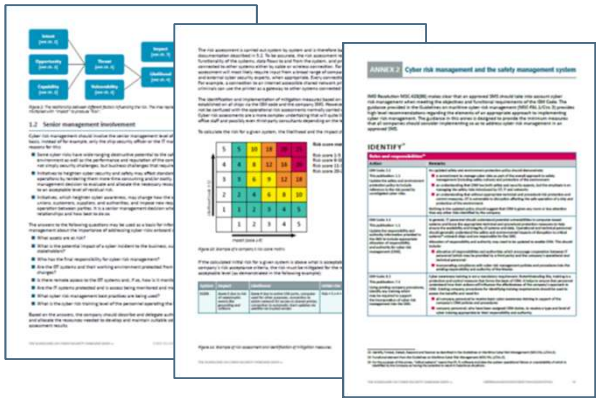
Contents

Chapter 1 – Overview of cyber security risk management

Chapters 2-5 – Assessment of cyber security risks

Chapters 7-8 – Development of security controls

Chapters 9-10 – Guidance on response and recovery



Excerpts from BIMCO guidelines v4

https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

BIMCO Guidelines key highlights

- Clear mapping between ISM Code and guidelines
- Mandate for senior management involvement
- Relationships between owners, managers, agents and suppliers
- Examples of known incidents and risks
- Tailoring of best practice to maritime domain

Port state control - key points from USCG CVC-WI-027

The inspector shall identify when basic cyber hygiene procedures are not in place onboard.

- Poor cyber hygiene
  - Username / Password openly displayed
  - Computer system appears to require a generic login or no login for access
  - Computer system does not appear to automatically log out after extended period of user inactivity
  - Heavy reliance on flash drive/USB media use
- Shipboard computers readily appear to have been compromised by ransomware/excessive popups
- Officers/crew complain about unusual network issues and reliability impacting shipboard systems
- Unit/vessel screener received potential ‘spoofed’ email from master/crew onboard.

The inspector should evaluate whether or not a cybersecurity event was a factor in the failure of a system required for the safe navigation or operation of the vessel

- Decide if there it justification for more detailed inspection (exam)

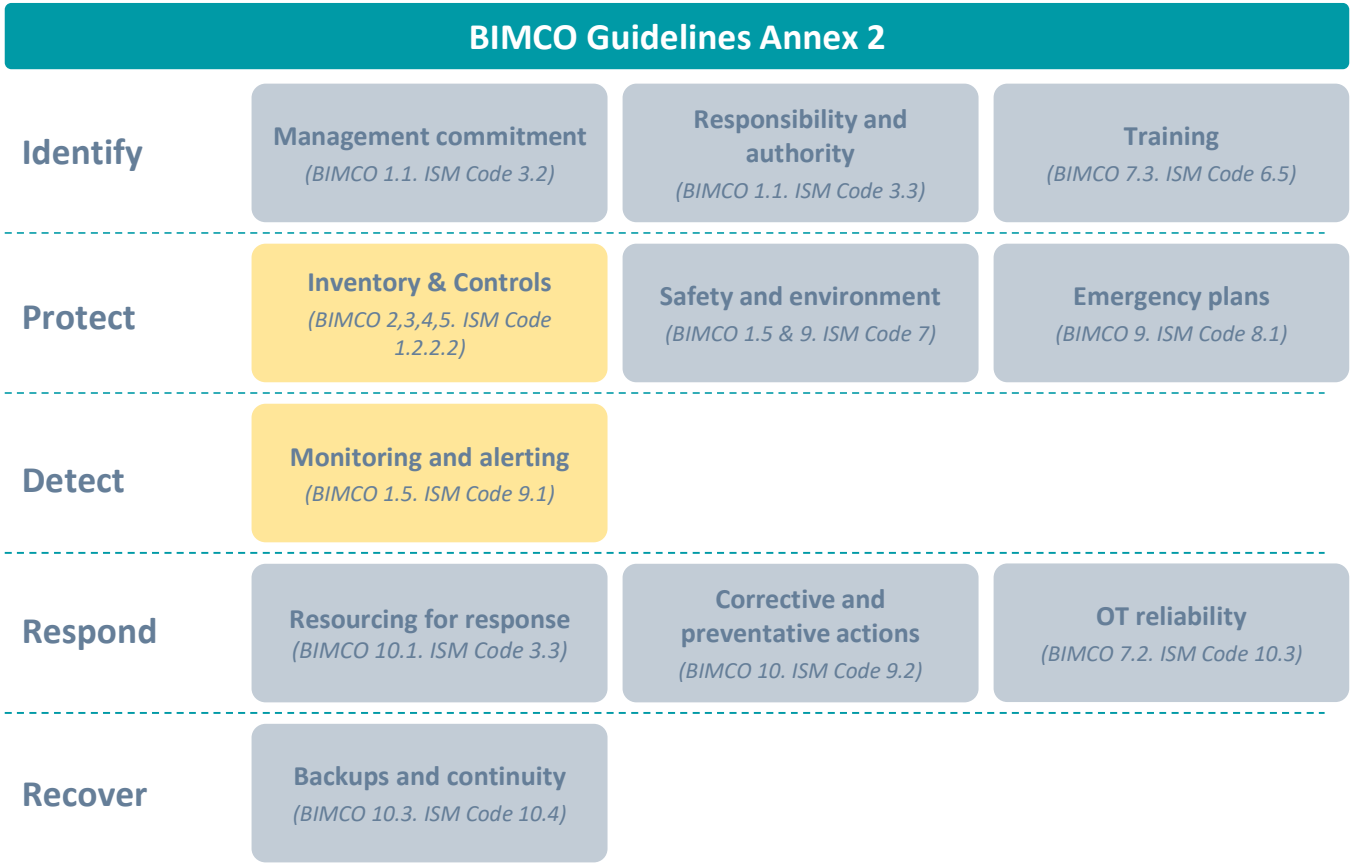
Regulation summary

- Vessels have increasing exposure to cybersecurity risks
- IMO Regulation introduced in January 2021
- Has broad implication for management of onboard systems
- BIMCO Guidelines help to interpret the regulation
- Initial audit requirements focused on basic hygiene factors

Cyber Security One Year Later

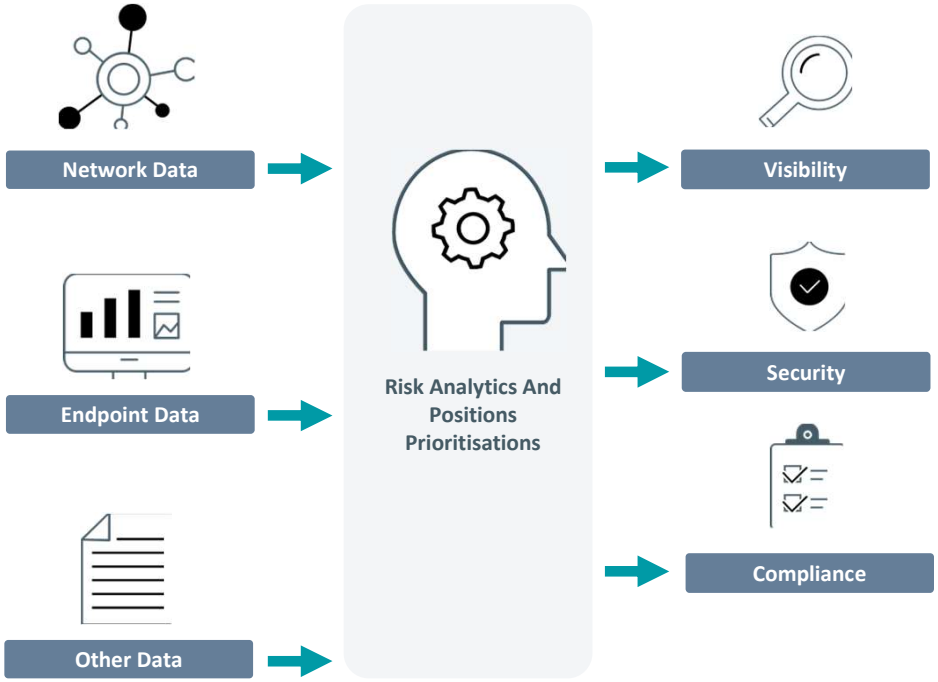
CYBEROWL

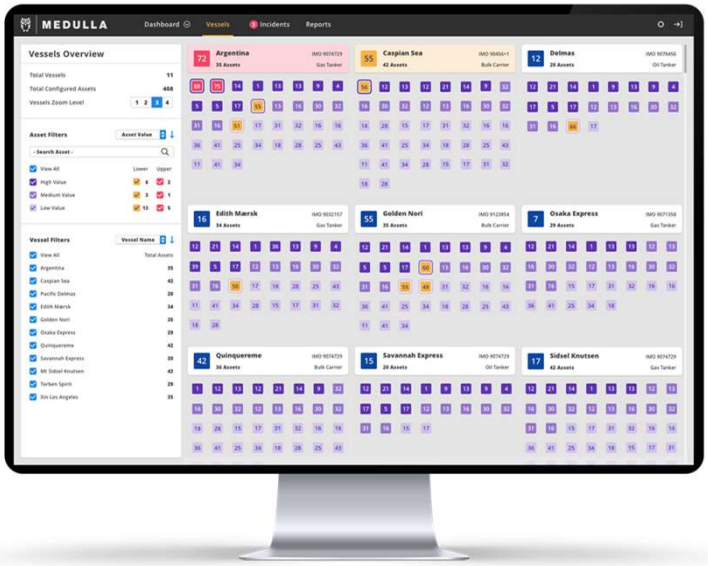
Key security domains (BIMCO Guidelines – Annex 2)



CyberOwl's perspective

We collect and analyse diverse sources of data from vessels:





And deliver data driven…

- Collection of inventory
- Risk assessment
- Validation of security controls
- Security monitoring
- Response recommendations

Inventory & Controls

Inventory discovery

- Operators have increasingly good visibility of connected devices
- Other types of inventory are more difficult to manage

Risk assessment

- Most operators have completed initial risk assessments
- But the results should be taken with caution

Application software security

- VSAT connectivity is allowing more frequent software updates

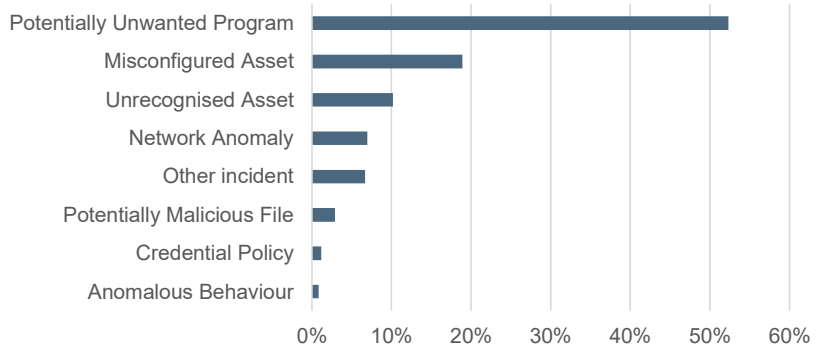
Secure configurations

- Hardening is difficult because crew still need flexibility
- Few easy options for improvement but monitoring can help

Monitoring & Alerting

Incident detection

- Majority of incidents are minor compliance issues
- Most malware incidents involve USB devices



Proportions of incidents raised by CyberOwl

Driving forces for further progress

- Availability of security tools tailored to marine requirements
- Industry benchmarking initiatives
- Class notations and type approvals
- Insurance and supply chain pressure
- Inspections and audit

Progress summary

- Good progress on inventory and patching
- Risk assessments have focussed minds but will need refreshing
- Some difficult challenges remain especially with OT and crew autonomy
- There are several driving forces that will deliver further improvement
- Inspections will get tougher

Cyber security and piracy

Cyber security and piracy – threat convergence?

Cyber security and piracy – actors

Piracy threat actors

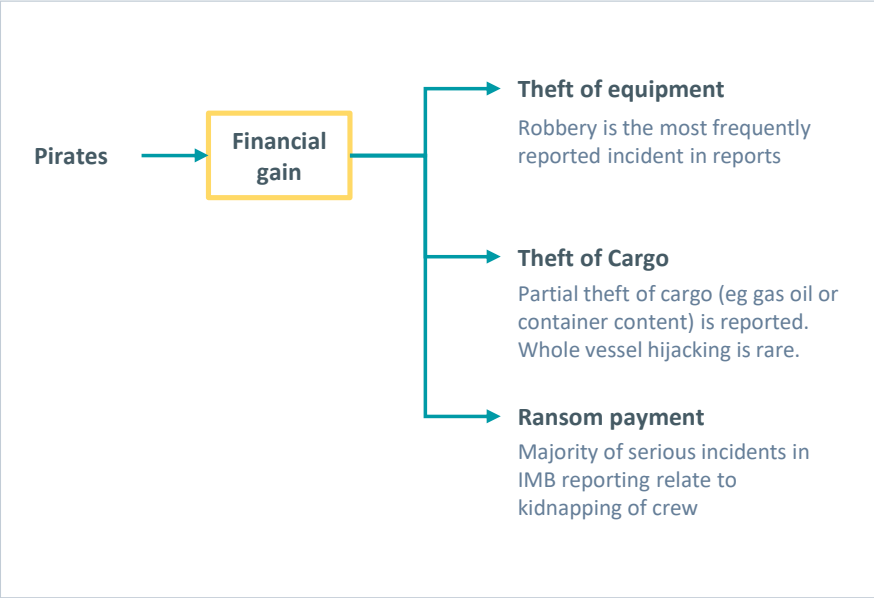
- Characterised by area
- Constrained geographically
- Physical
- Prepared to use violence

Cyber threat actors

- Characterised by motivation
- Global
- Technical
- Seek to minimise risk

Cyber security and piracy – motivations

Piracy threat motivations



Summary assessment of motivations in reporting by ReCAAP, IMB etc

Cyber threat motivations

Group	Motivation
Accidental actors	■ No malicious motive but still end up causing unintended harm through bad luck, lack of knowledge or lack of care, eg by inserting infected USB in onboard IT or OT systems.
Activists (including disgruntled employees)	■ revenge ■ disruption of operations ■ media attention ■ reputational damage
Criminals	■ financial gain ■ commercial espionage ■ industrial espionage
Opportunists	■ the challenge ■ reputational gain ■ financial gain
States **State sponsored organisations** **Terrorists**	■ political/idealogical gain eg (un)controlled disruption to economies and critical national infrastructure ■ espionage ■ financial gain ■ commercial espionage ■ industrial espionage ■ commercial gain

List of cyber security threat actors included in BIMCO guidelines

Cyber security and piracy – methods

Cyber “kill-chain”

Piracy “kill-chain”

Cyber security and piracy – methods

Similarities in methods between cyber threats and piracy threats:

- Use of extortion
- Persistent
- Adaptable and imaginative
- Asymmetric
- Supporting ecosystem

Cyber security and piracy – convergence

Piracy “kill-chain”

Potential cyber attack synergies

Identify high value target
- Use of AIS data

Identify accessible target

Identify target containers
- Cyber attack on port systems
- Cyber attack on cargo systems

Locate target
- Use of AIS data

Cause target to slow
- Send AIS man overboard alert
- Cyber attack on propulsion

Cause target to near shore
- GPS spoofing
- Cyber attack on navigation

Approach undetected
- Spoof AIS to confuse crew
- Cyber attack on radar systems

Board undetected
- Cyber attack on CCTV systems
- Cyber attack on alarm systems

Prevent countermeasures
- Cyber attack on alarm systems
- Cyber attack on access control

Access restricted areas
- Cyber attack on access control

Frustrate rescue
- Damage comms systems
- Cyber attack on comms systems

Alternate monetisation
- Install ransomware
- Steal cargo data

Cyber security and piracy

How soon might we see converged attacks?

No evidence that pirates will quickly obtain advanced skills

- There is limited off-the-shelf capability to target vessels
- Even relatively simple techniques like AIS spoofing will require planning and coordination to be effective
- But there are many cyber criminals who operate on a ‘hack for hire’ basis and could be paid by pirates for their support if it was economically viable

Cyber threat actors could pay pirates for physical access

- A pirate could be paid to connect a USB drive while onboard a vessel in order to circumvent network controls
- Could become an overlap between piracy and state-sponsored cyber attacks

Cyber security and piracy – leading indicators and initiatives

Threat intelligence sharing for

- Developing “business models” of piracy gangs
- Evidence of use of AIS or other data
- Availability of accessible malware targeting ships systems
- Signs of network or system access during an attack
- Cyber attacks with geographic focus

Cyber security and piracy summary

There are similarities between cyber attacks and piracy

But also important differences

Cyber attacks could enable more successful piracy

But the economics and skills required mean this may not happen

The industry must watch for any developments

Conclusions

Cyber security in marine has a long way to go

Regulation has started to result in real progress

Important to mitigate potential threat of cyber and piracy convergence

CYBEROWL

Russell Kempley

Chief Security Officer

russell.kempley@cyberowl.io

cyberowl.io

/company/cyberowl

Visibility | Security | Compliance