CYBEROWL

Developing a fleet cyber security operations that works

Digital Ship Oslo
7 July 2023

Visibility | Security | Compliance

Introducing CyberOwl

Deep expertise in maritime sector

Award-winning technology

National Cyber Security Centre
a part of GCHQ
Cyber Accelerator Alumni

GCHQ
Cyber Accelerator Alumni

Maritime UK Awards
10.03.22 Glasgow

2021 Cyber Security Award
SMART4SEA
Shortlisted

Seatrade Awards
In association with Lloyd's List
Finalist

LLOYD'S
Science of Risk Prize

finalist
Cyber Security Awards

Trusted by customers globally

EASTERN PACIFIC SHIPPING

PIL

PCL

CMB

SWIRE SHIPPING

NAVARONE S.A.

aet

ANGLO-EASTERN

LEMISSOLER

Andriaki

ELETSON

TUFTON

We help fleet operators

Know what you have onboard

Keep it secure

Prove you have secured it

Delivered through:

Proprietary network sensor, agent and analytics technology

24x7 SOC analysts in the UK and Singapore

Specialist maritime cybersecurity consultants

In collaboration with: HFW

Office / enterprise cyber security operations

=

Vessel / fleet cyber security operations

Office / enterprise cyber security operations

???

Vessel / fleet cyber security operations

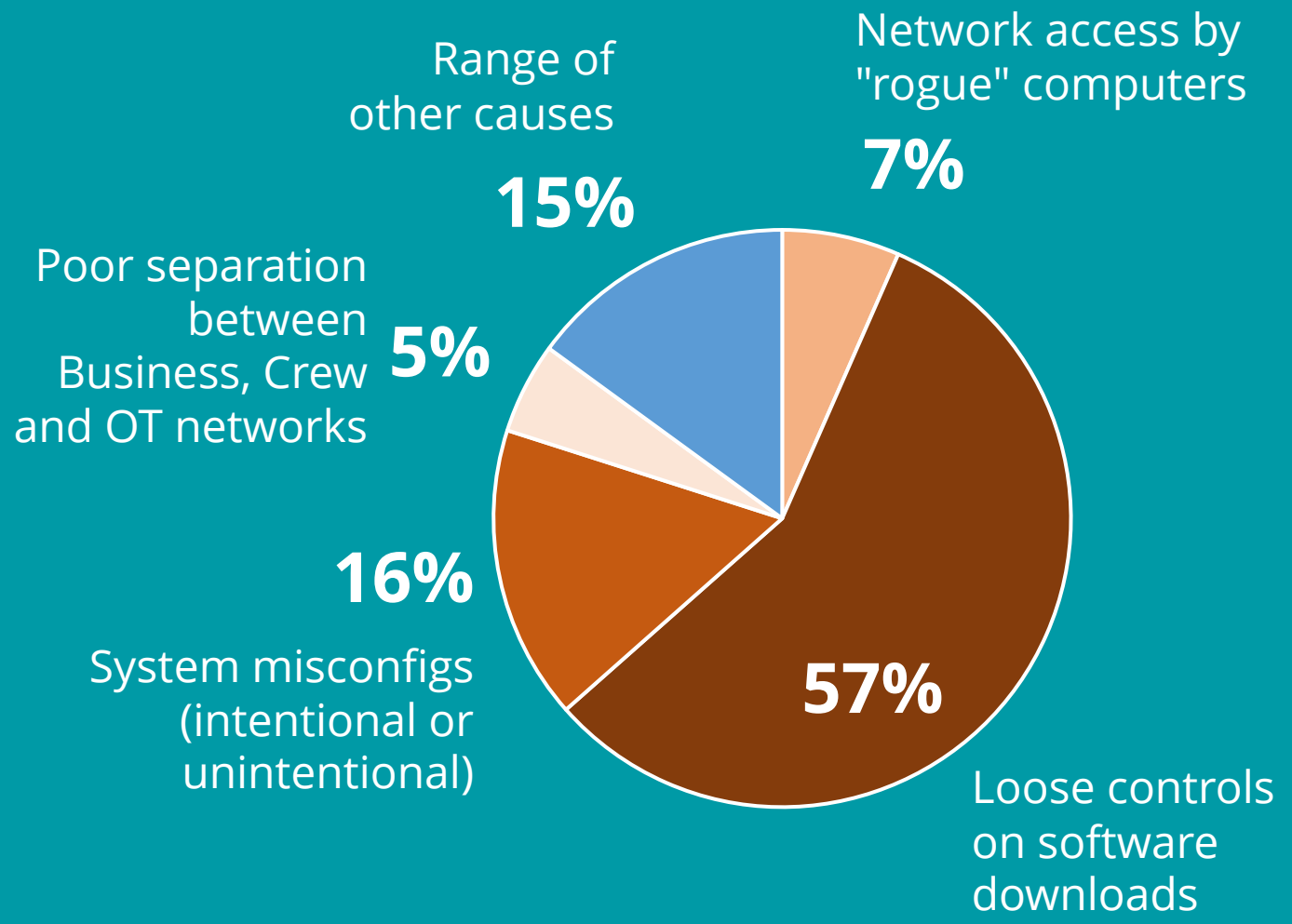
Nature of the risks…

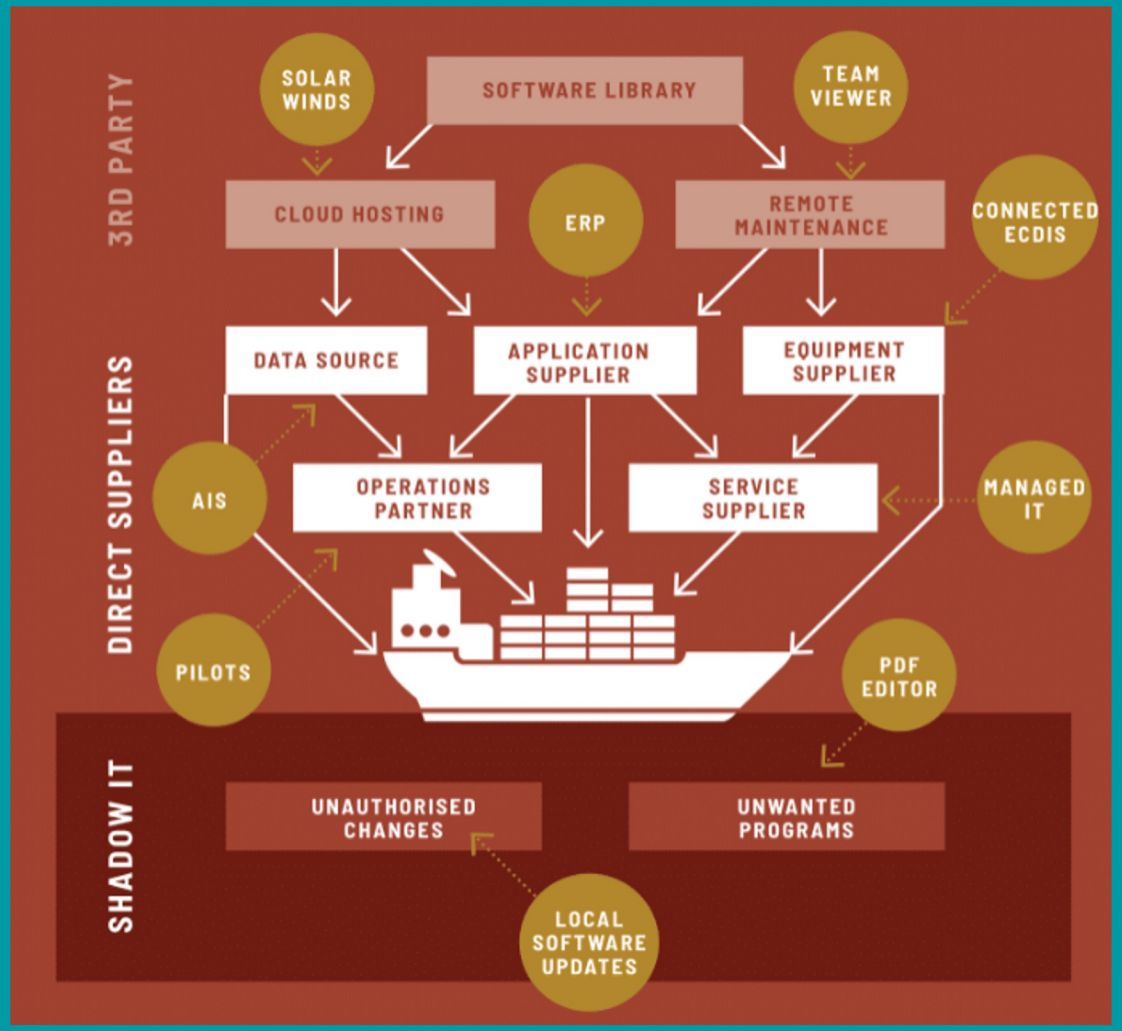
…are a bit different

A typical fleet of 50 vessels experiences 70-80 cyber incidents a year

These risks link directly back to:

- **Lack of visibility**
- **Poor implementation of controls**
- **Human error**

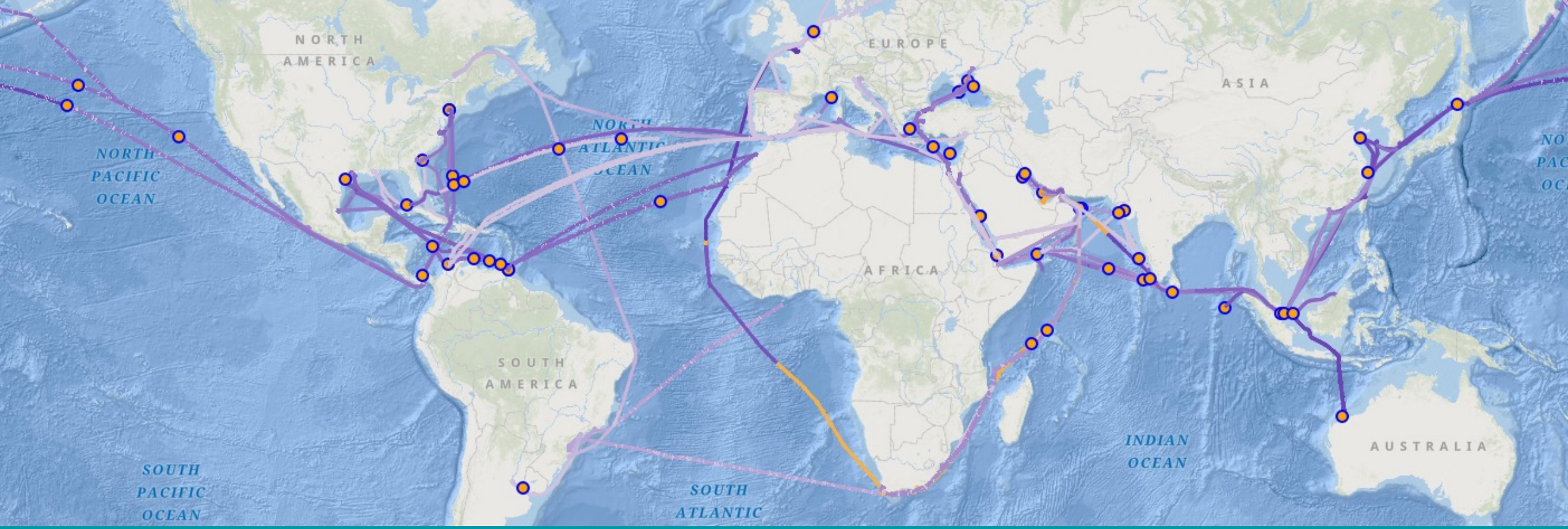




50%+ *ships have 40-180 connected devices*

60% *onboard computers have unapproved software*

30% *fleets give full local admin rights to crew*



80%+

cyber incidents raised shortly after vessel leaves port

The options for controlling these risks…

…are a bit different

ISPS Code:

Master has the overriding authority and responsibility to make decisions with respect to the safety and security of the ship

Typical approaches:

Local admin privileges

Completing operations trumps security

The way you handle response...

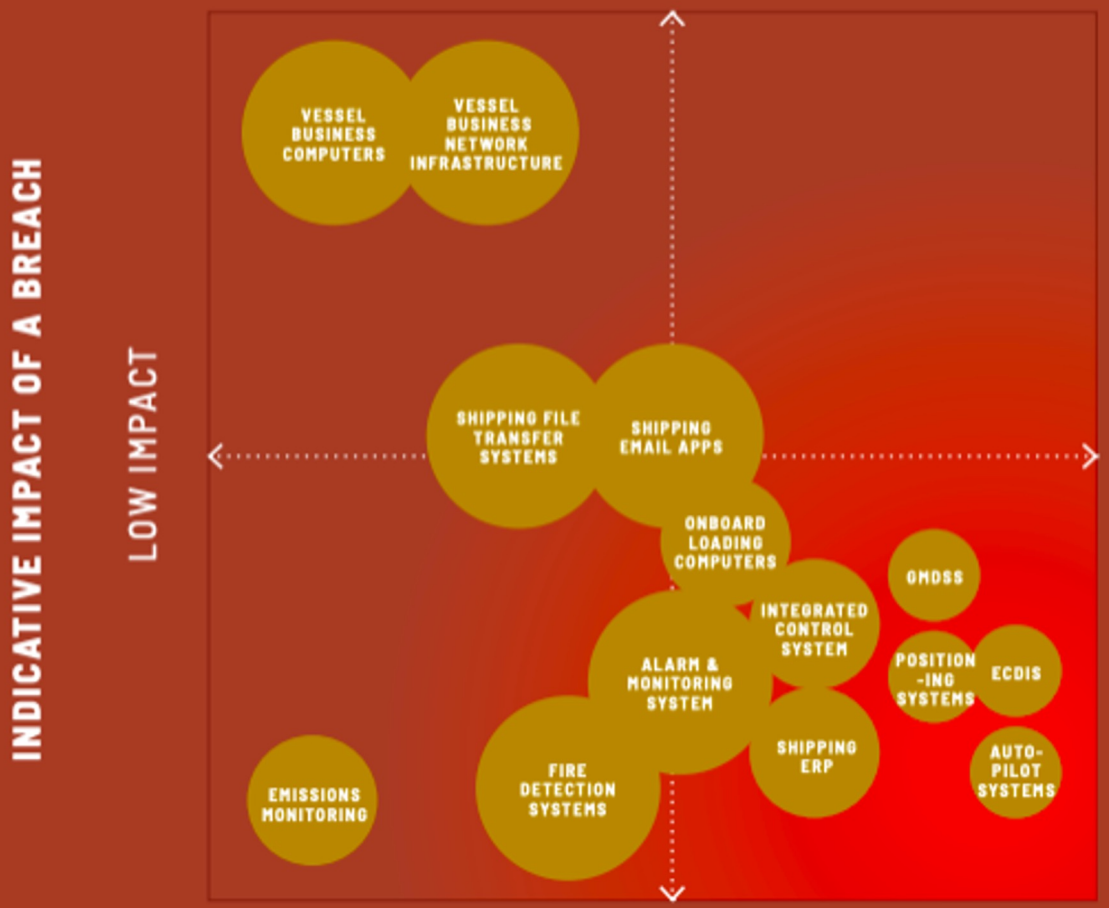
...is a bit different

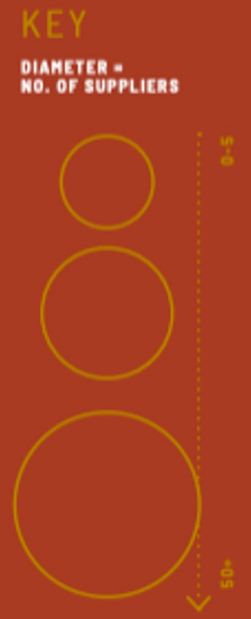
70%

of vessel cyber incident response involves more than the IT team

SHIPOWNER'S CONTROL OVER SECURITY

(dependent on specific operations of vessel)





So how do you develop a fleet cyber security operations that works?

1. Involve people who understand fleet operations in your SecOps team

1. Involve people who understand fleet operations in your SecOps team
2. Choose controls that do not block fleet operations

1. Involve people who understand fleet operations in your SecOps team
2. Choose controls that do not block fleet operations
3. Enable visibility to maximise support from shore

1. Involve people who understand fleet operations in your SecOps team
2. Choose controls that do not block fleet operations
3. Enable visibility to maximise support from shore
4. Engage crew in basic incident response

1. Involve people who understand fleet operations in your SecOps team
2. Choose controls that do not block fleet operations
3. Enable visibility to maximise support from shore
4. Engage crew in basic incident response
5. Build muscle memory through cyber exercises

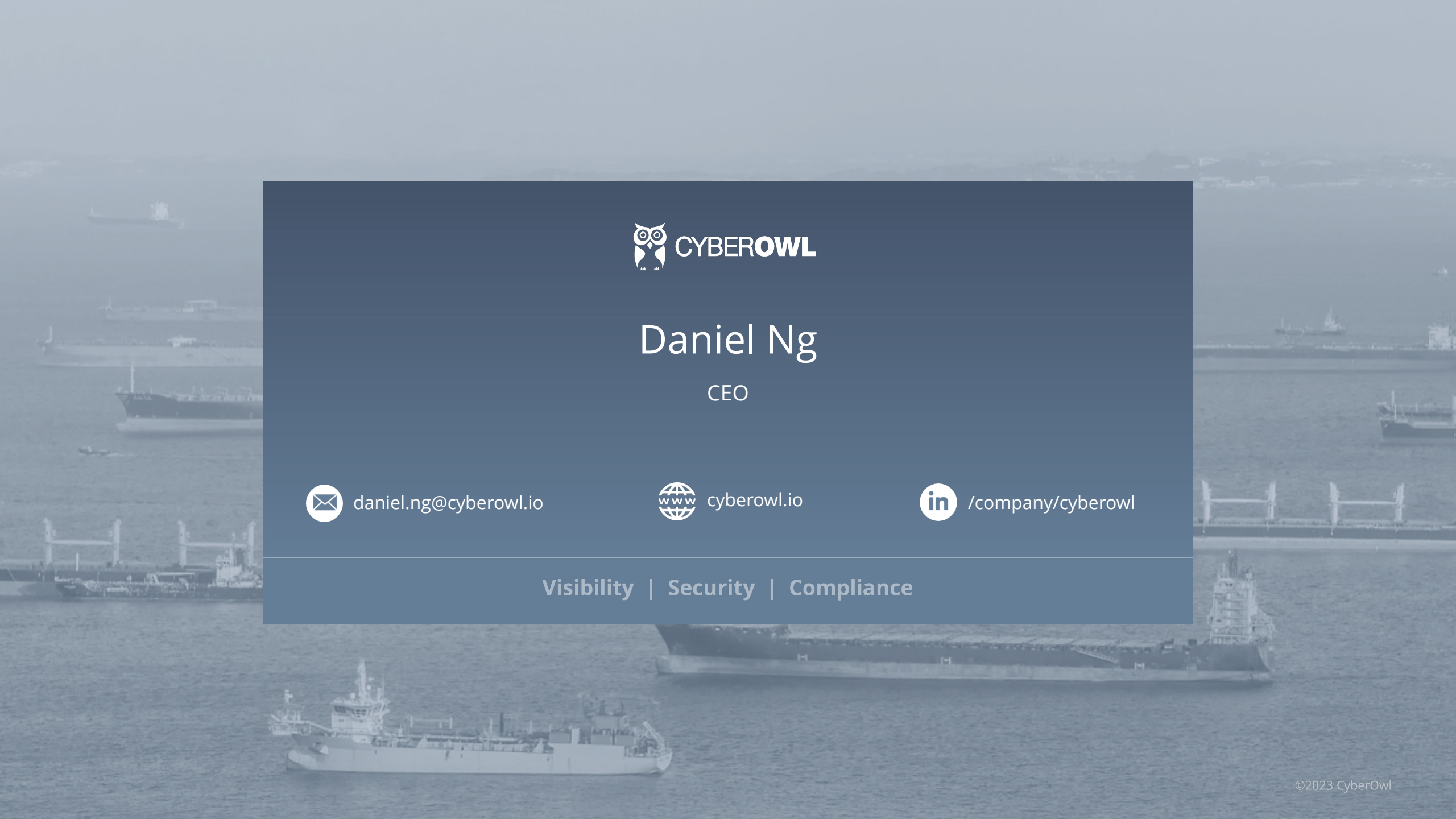
Ask us for more benchmarks on vessel cyber security:

Daniel Ng

Chief Executive Officer

Richard Wagner

Regional Director, APAC



CYBEROWL

Daniel Ng

CEO

daniel.ng@cyberowl.io

cyberowl.io

/company/cyberowl

Visibility | Security | Compliance