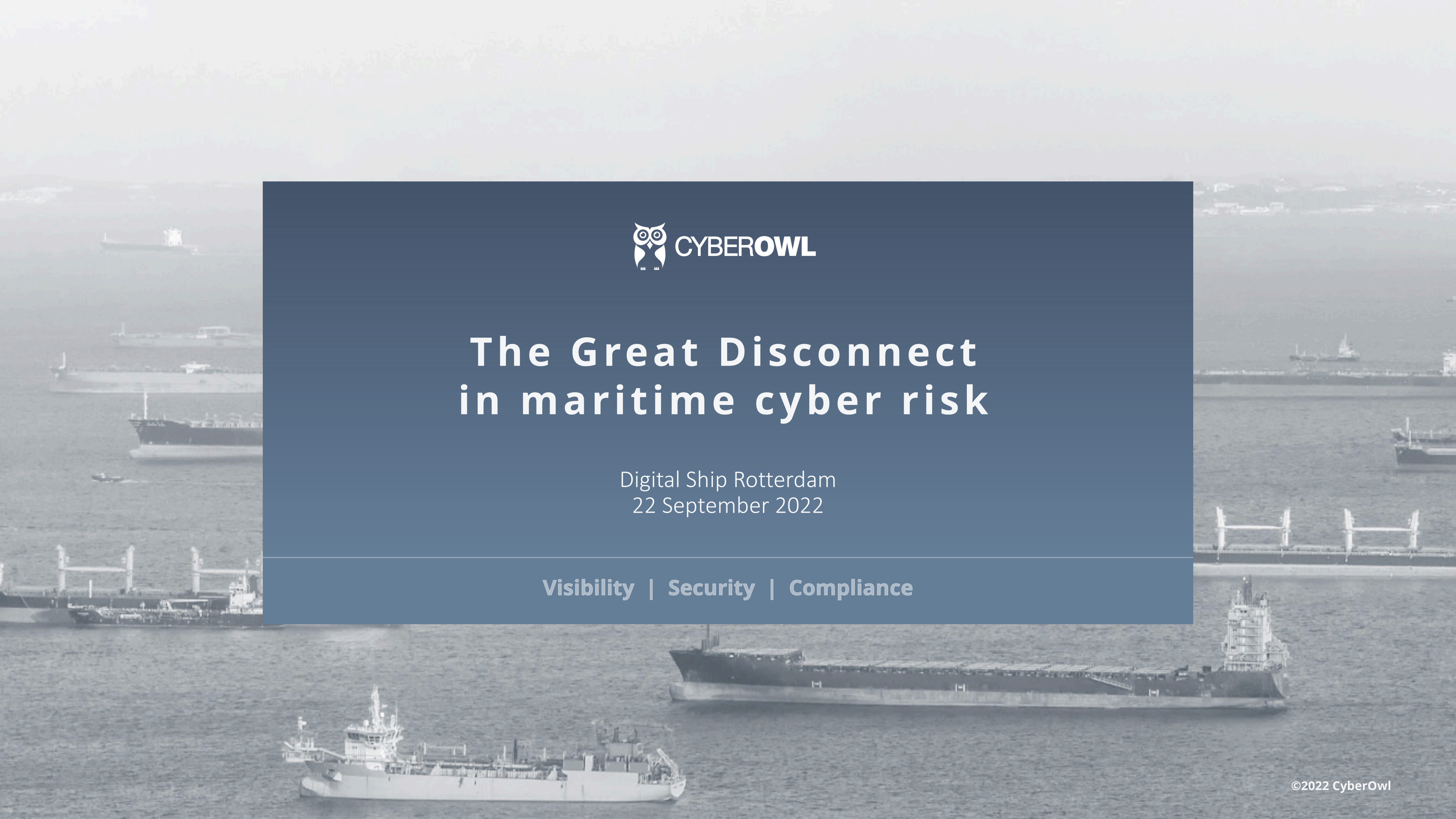


CYBEROWL

The Great Disconnect in maritime cyber risk

Digital Ship Rotterdam
22 September 2022

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

misc

SWIRE SHIPPING

NAVARONE S.A.

aet

TUFTON

ZEABORN SHIP MANAGEMENT

Andriaki

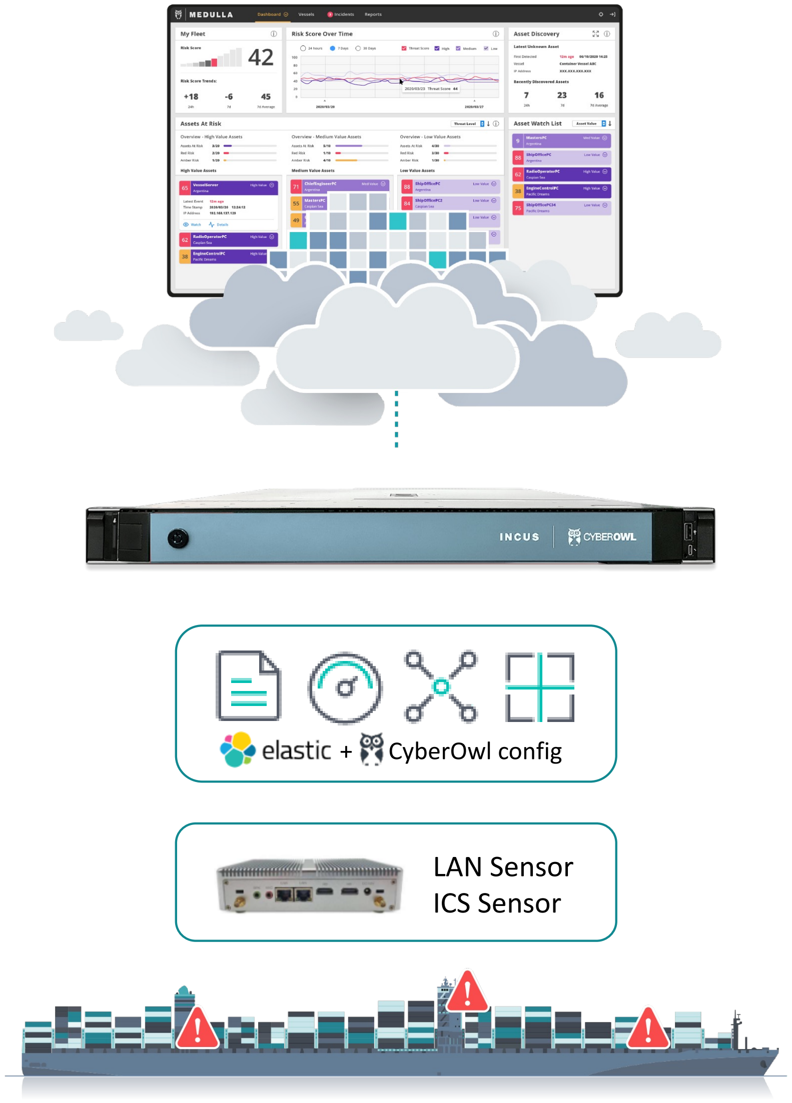
ELETSON

We help fleet operators

Know what you have onboard

Keep it secure

Prove you have secured it



THE GREAT DISCONNECT

The state of cyber risk management in the maritime industry

Nick Chubb, Patrick Finn & Daniel Ng

Foreword by Guy Platten, Secretary General of the International Chamber of Shipping

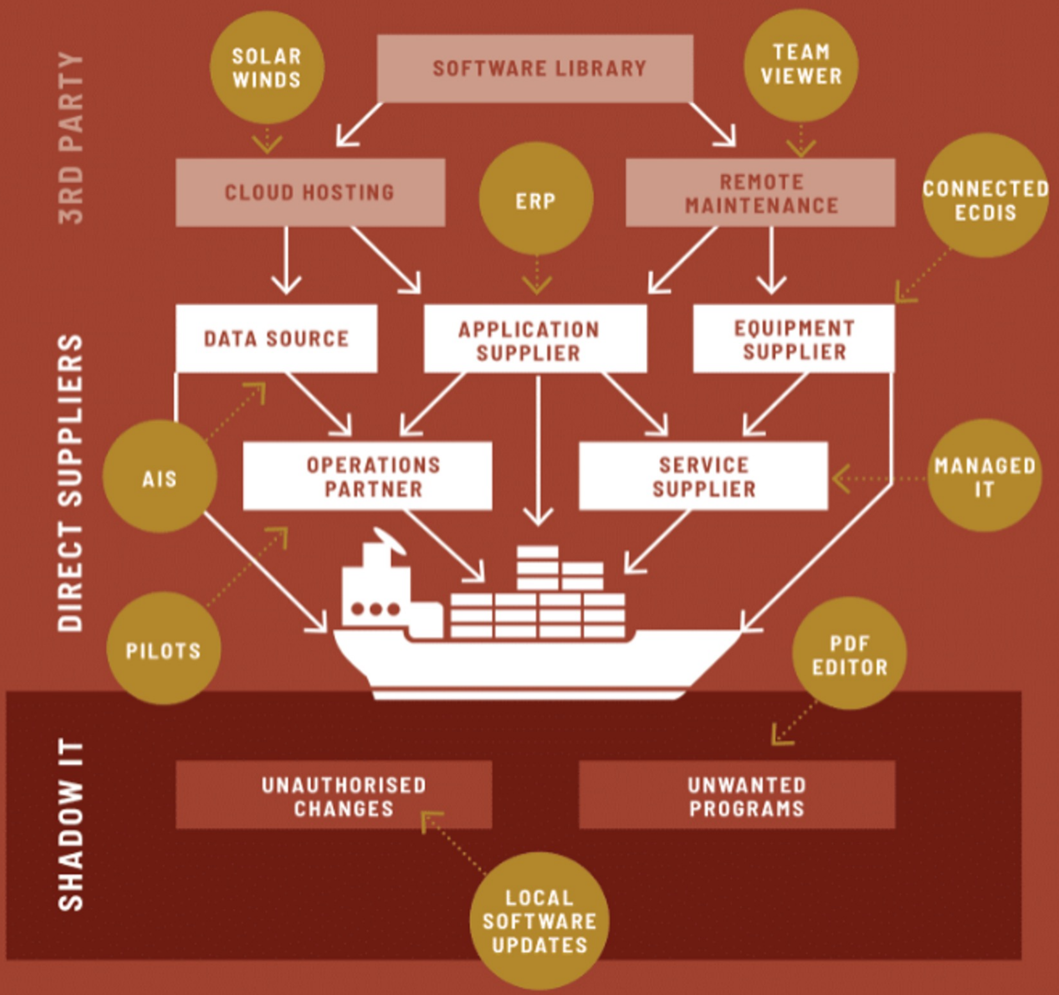
combining insights from:

200 *shipping experts*

80 *fleets*

Data from vessels CyberOwl monitors

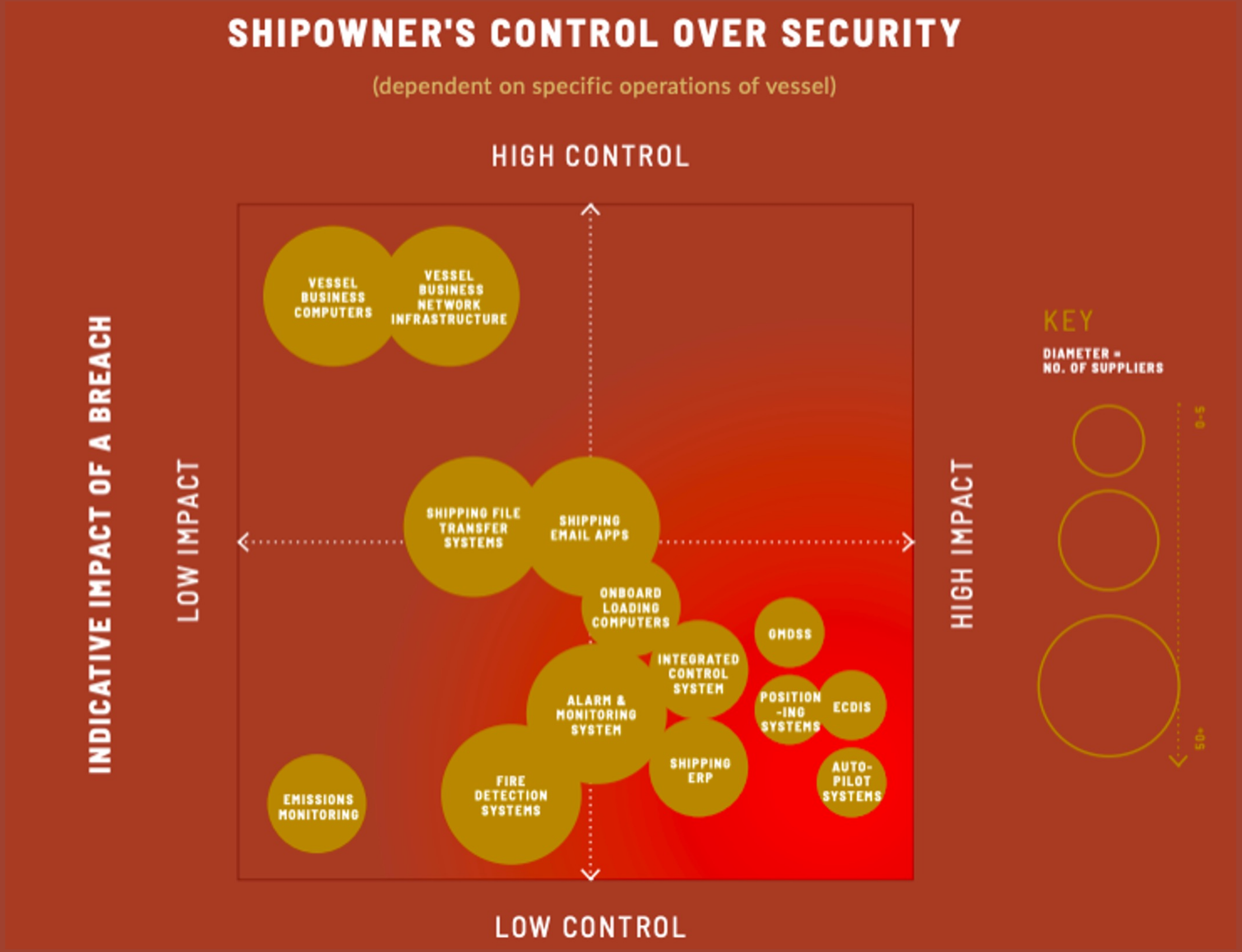
The supply chain disconnect



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

60% *onboard computers have unapproved software*

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



SHIPOWNER'S CONTROL OVER SECURITY

(dependent on specific operations of vessel)

only

65%

vessel systems suppliers asked to prove cyber risk management

Vessels with at least one critical machine frequently:

Tethered:	*As hotspot:*	*On wifi:*
8%	**16%**	**28%**

Case study: Nation-state malware on a fleet of commercial vessels

- **8 vessels, 2 fleets, same malware**
- **Same strain on both IT and OT systems**
- **Malware provides actor full control of machine**
- **Main preventative control for OT systems was internet connectivity**

The risk disconnect

3% *of cyber attacks resulted in the respondents' organisation paying a ransom.*

$3.1 MILLION *...Is the average ransom paid* *only*

34%

believe their shipping organisation has appropriate insurance in place to cover cyber attacks

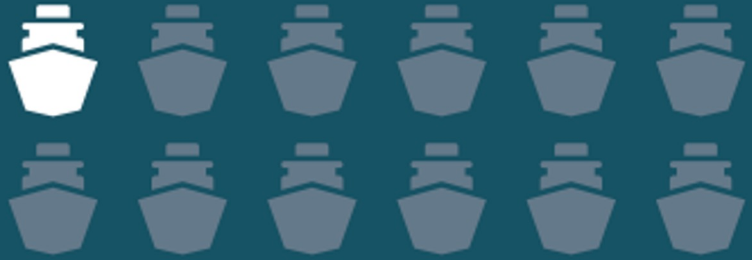
54%

of shipping companies spend less than $100K per year on cyber security management.

VS

$182,000

An average, cyber attacks cost ship operators $182,000 per year.

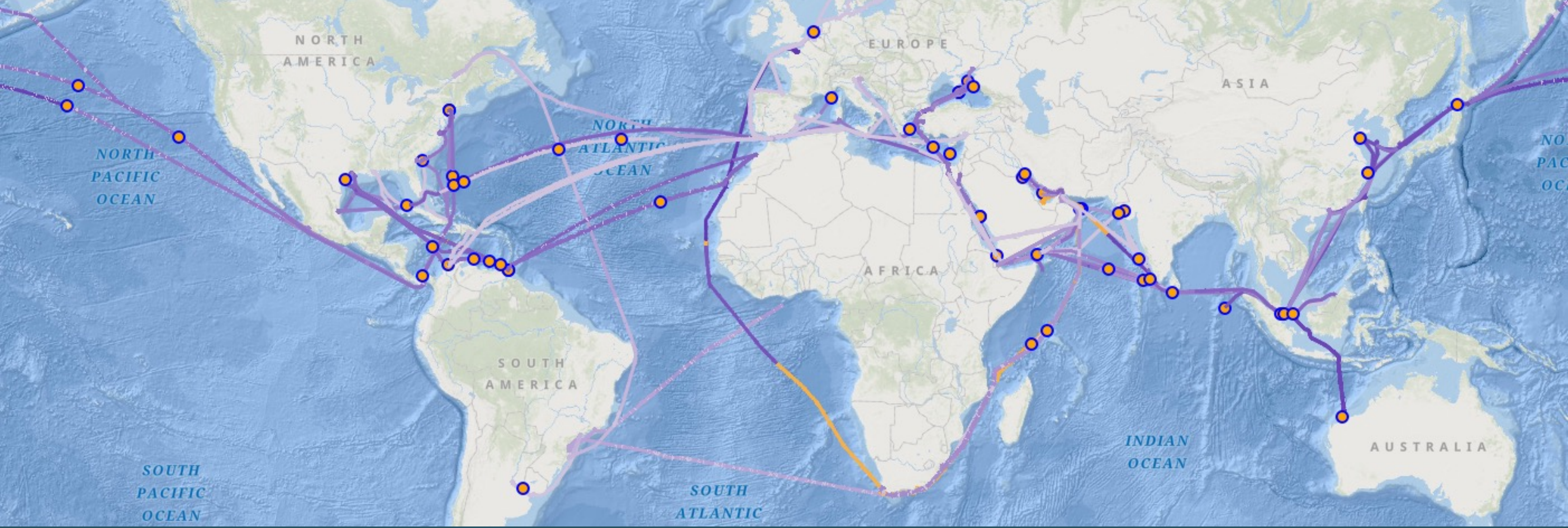


For 1 in 12 ship operators (8%), the average cost of cyber attacks is:

$1.8MILLION

PER YEAR

CYBEROWL



80%+

cyber incidents raised shortly after vessel leaves port

Recommendations to industry

1. Set up a dedicated cyber security directorate within fleet operations that covers both IT and OT security

2. Implement a comprehensive cyber incident training and drill programme

3. Develop minimum security standards for suppliers and partners

4. Conduct an urgent review of insurance policies and seek legal guidance on ransom payments

Join the maritime cyber security ecosystem we develop and maintain

We helped write the guidance

THE GUIDELINES ON
CYBER SECURITY ONBOARD SHIPS

Produced and supported by

BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), InterManager, International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Union of Marine Insurance (IUMI), Oil Companies International Marine Forum (OCIMF), Superyacht Builders Association (Sybass) and World Shipping Council (WSC)

v4

We maintain one of the world's largest maritime cyber risk sharing communities

200+

Shipping IT Directors meeting monthly

We lead maritime industry bodies to drive industry collaboration

SSA SINGAPORE SHIPPING ASSOCIATION

CyberOwl chairs the SSA Cybersecurity Subcommittee

We brief the insurers

IGP&I International Group of P&I Clubs

UKP&I

HELLENIC WAR RISKS

Join our upcoming workshops

MIND THE GAP
BRINGING THE SHIPPING COMMUNITY TOGETHER TO BRIDGE THE GREAT DISCONNECT IN MARITIME CYBER RISK MANAGEMENT

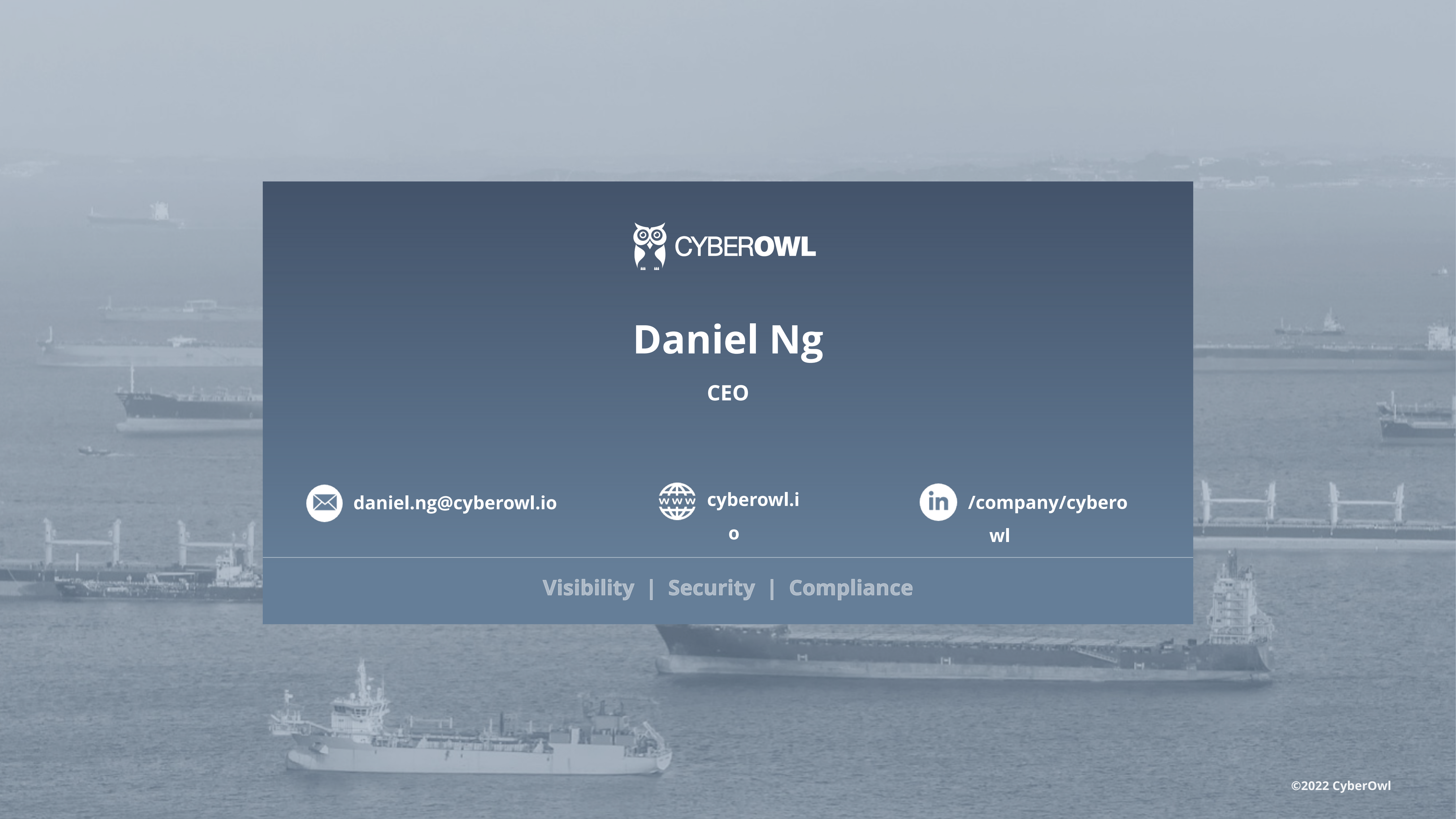
1 **Setting up a fleet SOC - "Cybersecurity operations on a shoestring budget**
Thursday, 13 October 2022, 8.00 am BST

2 **Decisions under fire - Practical maritime cyber exercise**
Thursday, 10 November 2022, 8.00 am London Time

3 **"Weaponising" compliance - turning compliance from foe to friend**
Thursday, 1 December 2022, 8.00 am London Time

Register here

SCAN ME



CYBEROWL

Daniel Ng

CEO

✉ daniel.ng@cyberowl.io

cyberowl.io

in /company/cyberowl

Visibility | Security | Compliance