



Does practice make perfect?: The art of cyber incident exercising.

Digital Ship Hamburg
30 March 2023

Visibility | Security | Compliance

Introducing CyberOwl

Deep expertise in maritime sector



Trusted by customers globally



Award-winning technology

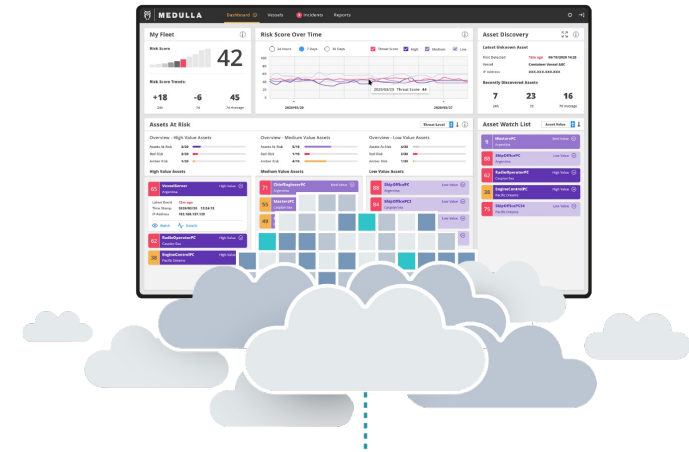


We help fleet operators

Know what you have onboard

Keep it secure

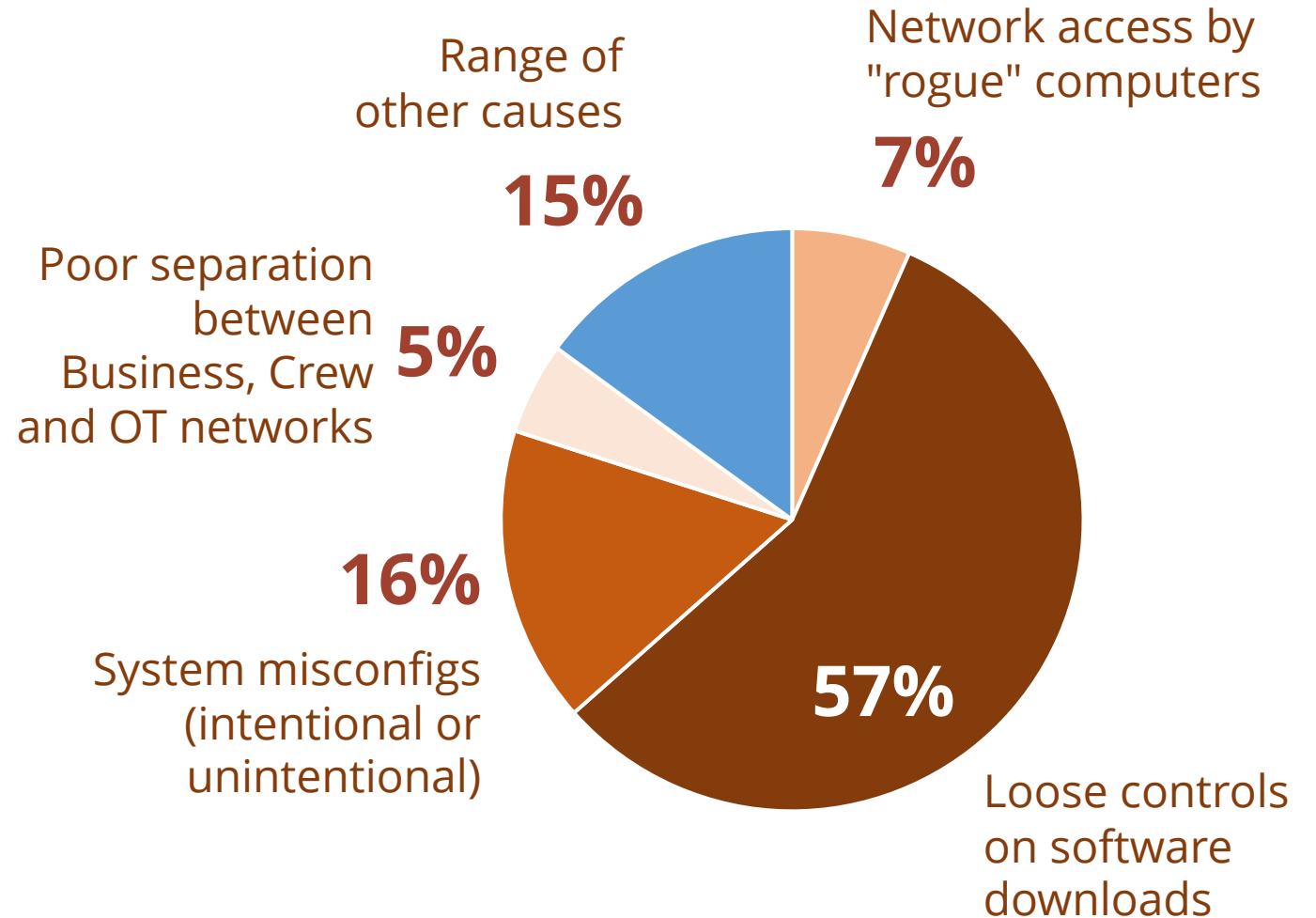
Prove you have secured it



**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**



70%

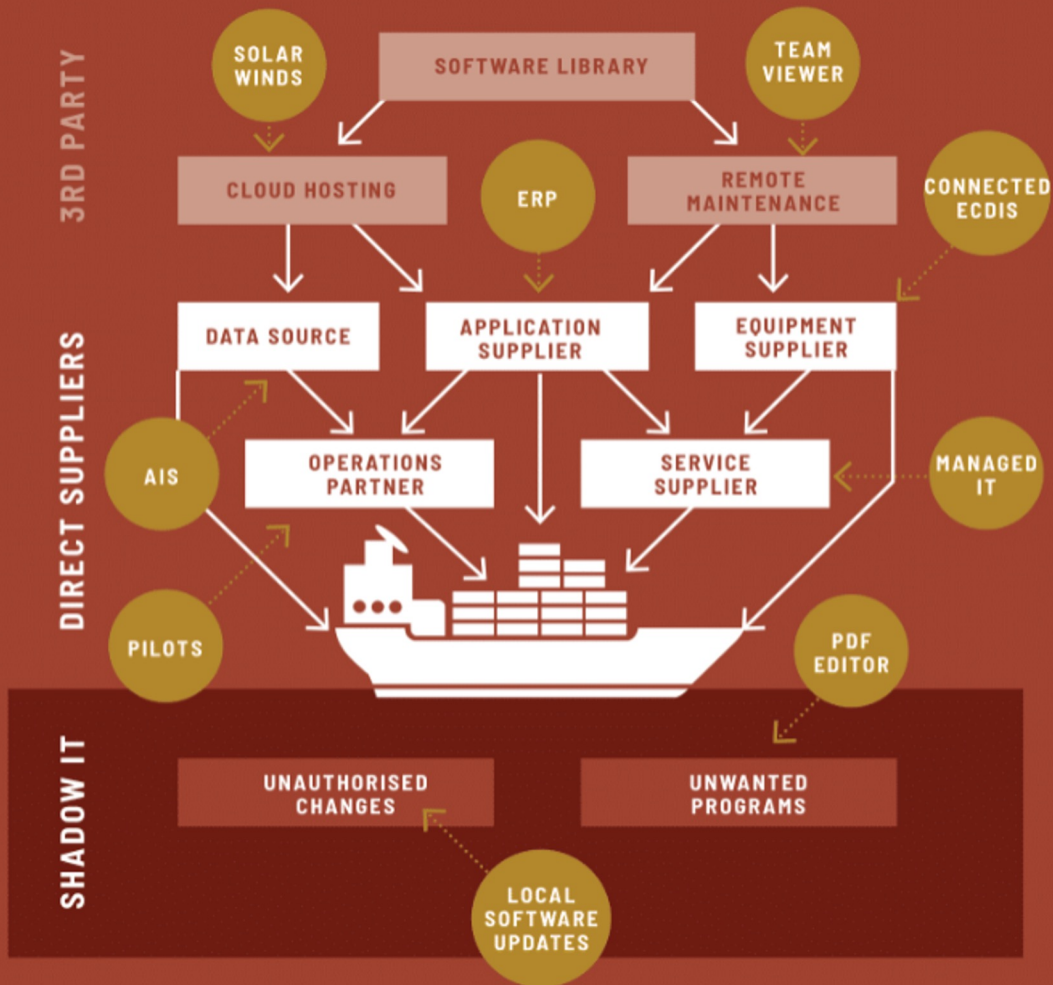
*of vessel cyber
incident response
involve more than
the IT team*

85%

*Seafarers do not
conduct regular
cyber exercises*

92%

*Shipping
executives do not
conduct regular
cyber exercises*



50%+

ships have 40-180 connected devices

60%

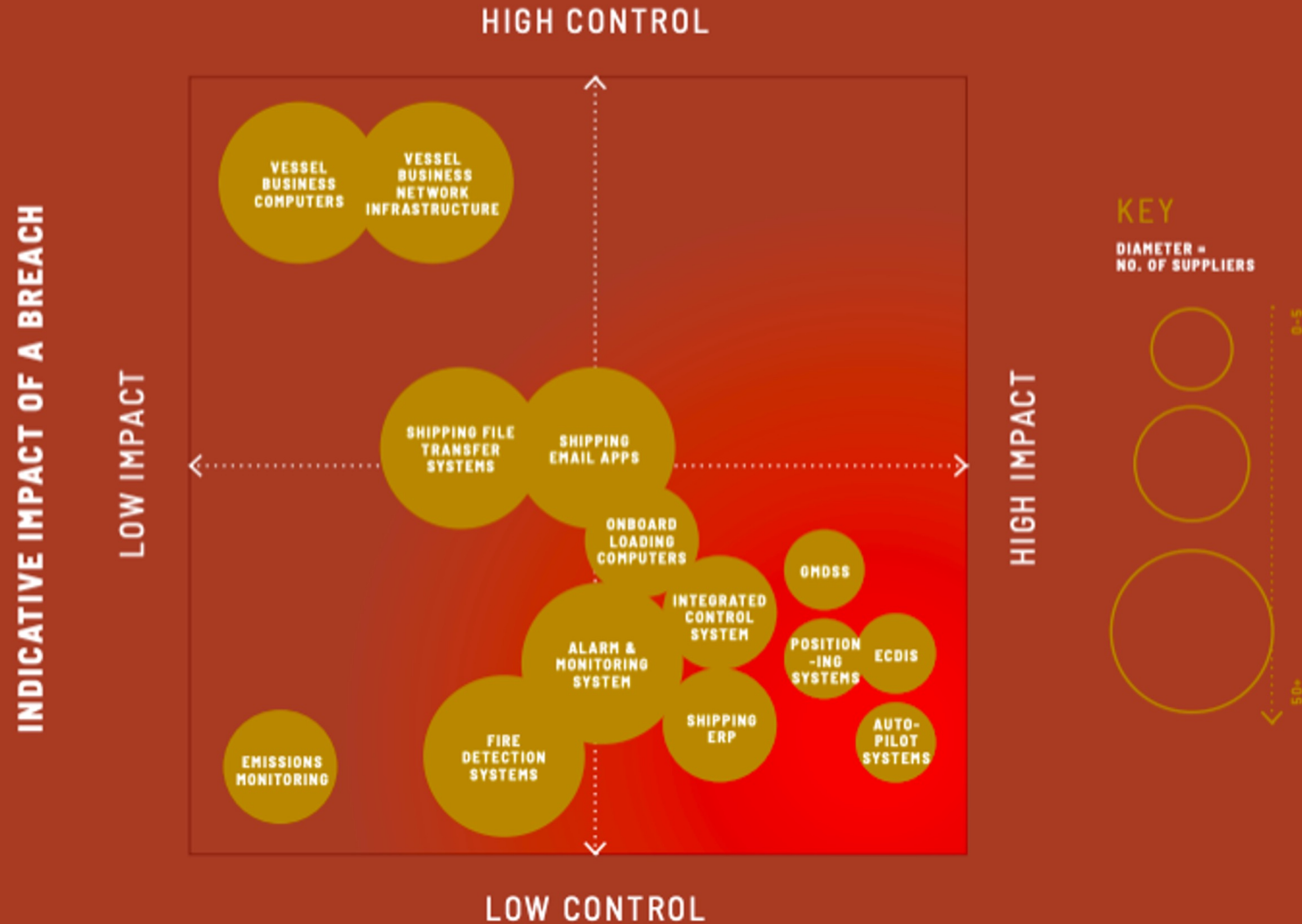
onboard computers have unapproved software

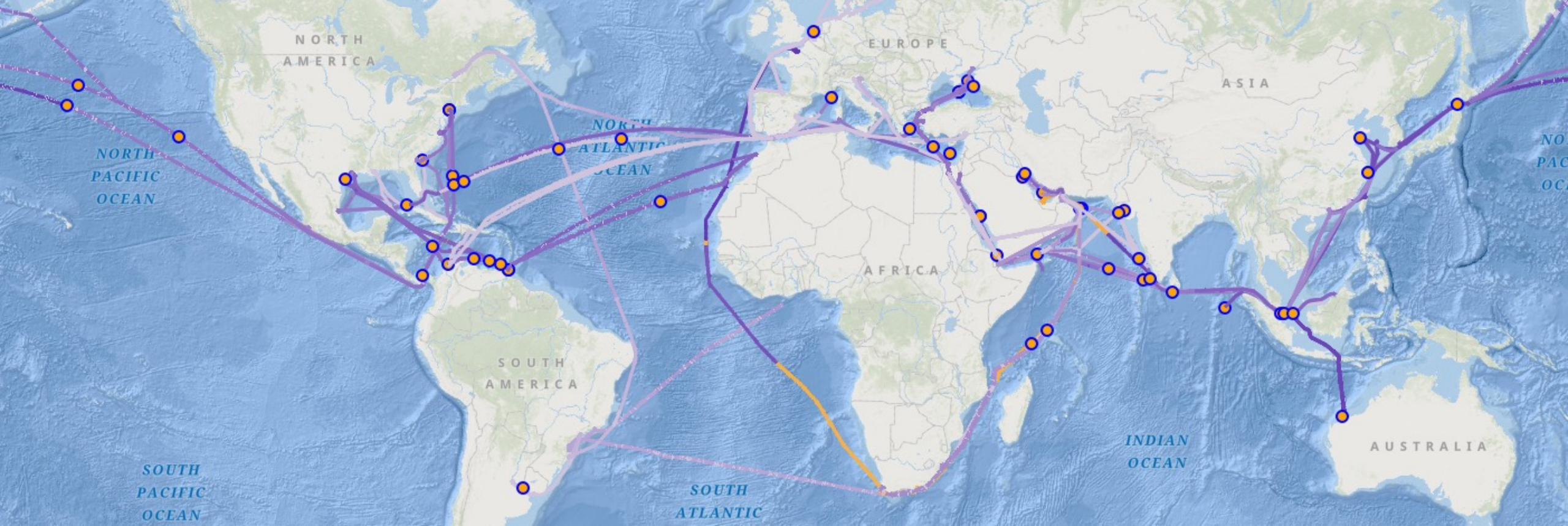
30%

fleets give full local admin rights to crew

SHIPOWER'S CONTROL OVER SECURITY

(dependent on specific operations of vessel)





80%+

cyber incidents raised shortly after vessel leaves port

0%

*Shipping operators
run cyber
exercises with
their key suppliers*

Dan Ng
CEO, CyberOwl



Chris Baars
Director Consulting





Chris' experience at MAERSK

The big incident





Chris' experience at MAERSK

**The big
incident**



**First few
exercises.
Zero budget.**



Chris' experience at MAERSK

**The big
incident**

**Launch of the Cyber
Security Operational
Readiness and Exercising
Department**



**First few
exercises.
Zero budget.**



Chris' experience at MAERSK

The big incident

Launch of the Cyber Security Operational Readiness and Exercising Department



**First few exercises.
Zero budget.**

Monthly exercises across the group

What changed?

1. Educated and engaged executives

What changed?

- 1. Educated and engaged executives**
- 2. Clarified roles and responsibilities**

What changed?

- 1. Educated and engaged executives**
- 2. Clarified roles and responsibilities**
- 3. Assessed adequacy of procedures**

What changed?

- 1. Educated and engaged executives**
- 2. Clarified roles and responsibilities**
- 3. Assessed adequacy of procedures**
- 4. Improved incident communication**

What changed?

- 1. Educated and engaged executives**
- 2. Clarified roles and responsibilities**
- 3. Assessed adequacy of procedures**
- 4. Improved incident communication**
- 5. Built muscle memory**

What changed?

- 1. Educated and engaged executives**
- 2. Clarified roles and responsibilities**
- 3. Assessed adequacy of procedures**
- 4. Improved incident communication**
- 5. Built muscle memory**
- 6. Evaluated insurance needs**

Some tips and tricks

1. Set objectives and corresponding metrics

2. A programme of exercise is better than one-offs

Exercising a tiered response structure

Bronze

TECHNICAL

- Activated first
- Performs rapid technical assessment of the incident
- Exercise using tooling under pressure

Silver

OPERATIONAL

- Activated first
- Conducts initial risk assessment
- Takes operational control of the incident and communication across response team

Gold

STRATEGIC

- Assumes overall command and strategic decision-making
- Considers wider business implications
- Handles external communication and media

3. Building the culture is everything

MIND THE GAP

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

**How do you work with your supply chain in a
cyber incident?**

*Thursday, 4 May 2023,
8.00 am BST / 10 am EEST / 3 pm SGT*

Register here



SCAN ME

WORLD TOUR EDITION

CYBERSECURE AT SEA 2023

WHO'S IN CHARGE?

Supporting partners



Standard Club
Part of NorthStandard



NORMA
CYBER



SCAN ME

Singapore

18 April

2.30 pm SGT

Hong Kong

10 May

2.30 pm HKT

Oslo

24 May

9.00 am CEST

Athens

13 June

2.30 pm EEST



Daniel Ng

CEO

 daniel.ng@cyberowl.io

 cyberowl.io

 [/company/cyberowl](https://www.linkedin.com/company/cyberowl)

Visibility | Security | Compliance