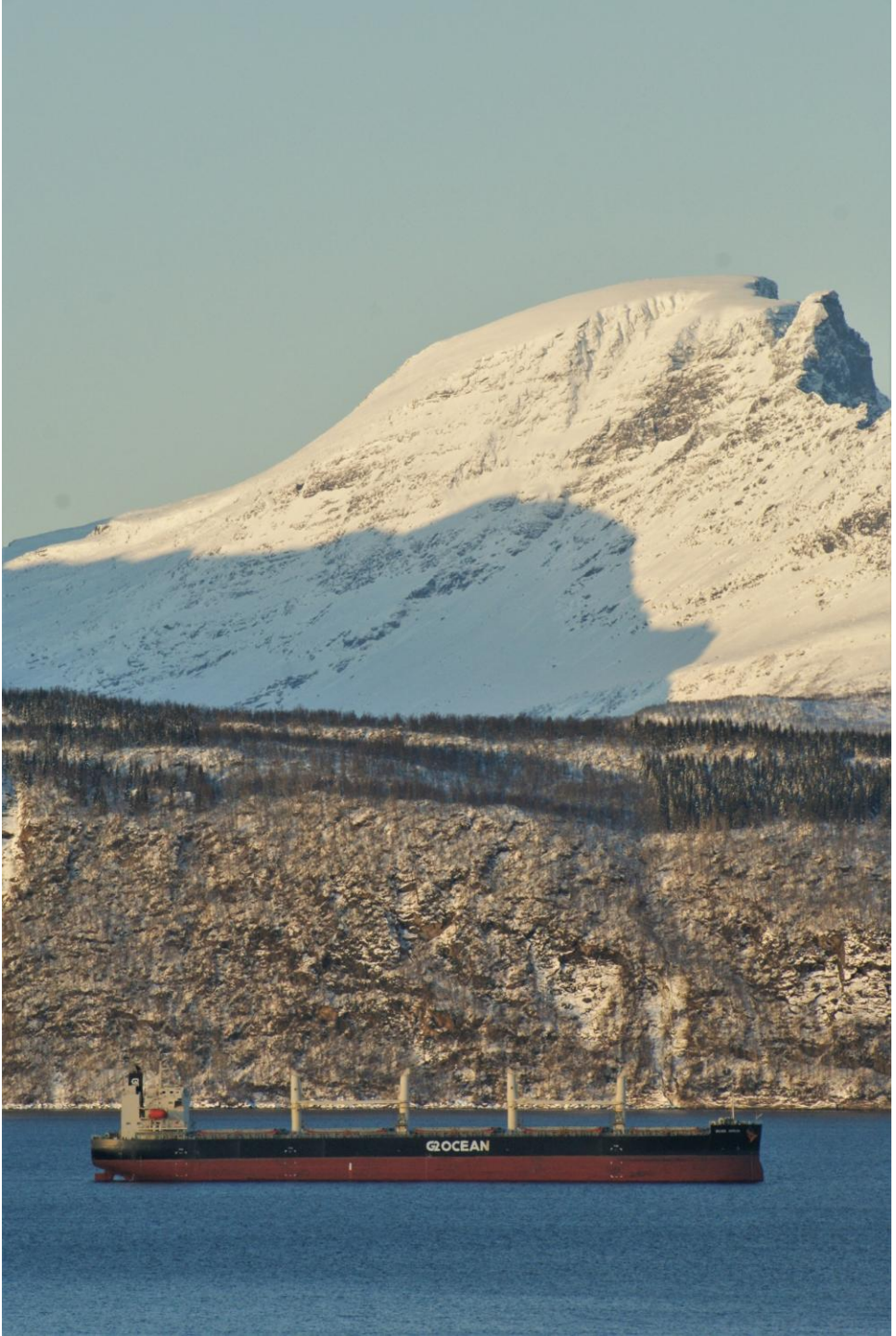
Managing the increasing cyber incident exposure

People Tech Maritime, Bergen 22 October 2026





Agenda

1. Increased fleet exposure
2. Identifying and focusing on highest risks
3. Incident readiness and business continuity
4. Importance of cyber insurance

1. INCREASED FLEET EXPOSURE

Vessels are increasingly exposed…

Fast, continuous connectivity

LEO satellites make every vessel internet-reachable

More data flows

OT data flows to shore and cloud, exposing OT to IT attacks

Remote access

Vendors and support teams patch and monitor from shore

…while AI shrinks the time to exploit

ATTACKERS

~72,000

CVEs expected in 2026, a new record

< 24 h

From vulnerability spotted to working exploit

DEFENDERS

30–60 days

Enterprise time to patch critical external CVEs

Source: Microsoft Digital Defense Report 2026

Severity scores need context

CVSS ALONE

One critical vulnerability on a low-impact asset will make a dashboard look red

IN CONTEXT

Several low and medium vulnerabilities on a critical or exposed service are the priority

Focus on what matters most

Safety-critical OT

One vulnerable device puts safety onboard at risk

Exposed & business critical assets

What attackers can reach from the internet, both ashore and at sea

Key suppliers

Critical third parties we depend on for our own business processes

3. ASSUME THE HIT

Expect the incident and get the business ready

Prevention has limits

Even strong, proactive defences won't stop every attack

AI-powered attackers

Stronger AI models cut the time, skill and cost of attacks

Third-party suppliers

Their systems and security practices are outside our control

Recovery goals

Continuity plans and recovery goals set with business owners

Exercises

Involve business owners in attack and outage scenarios

Fallbacks

Manual workarounds for long periods without a critical system

Crisis team

Trained, available, with clear authority and communication scenarios

Cyber insurance, a major asset during a crisis

Despite all preparation, an incident can highlight unexpected needs, limited staff availability, or missing specific in-house expertise

- Investigation and forensics experts
- Response capabilities
- Legal advice