MARITIME CYBERSECURITY & BRIDGE TEAM RESILIENCE

CHENNAI | JANUARY 2026

When Cyber Risk Meets the Reality of the Bridge

In maritime operations, there is no room for delay or ambiguity. Time and space are critical and when digital systems are compromised, the impact is immediate. Cyber incidents today are no longer confined to IT departments, they directly affect navigation, safety, and decision-making on the bridge. With this reality in focus, a two-day Maritime Cybersecurity and Bridge Team Resilience training program was conducted in Chennai in January 2026. The aim was simple yet urgent: move beyond awareness and build operational readiness across shipboard and shore-based teams. This training brought together sailing officers and shore IT professionals, reflecting how cyber incidents are actually handled, collaboratively, under pressure, and across locations.

Why This Training Was Needed?

As vessels become increasingly digital, the integration of IT and OT systems such as ECDIS, GPS, AIS, RADAR, and onboard networks, has expanded the cyber risk surface. Many incidents originate not from complex attacks, but from human fatigue, weak vendor controls, or delayed responses. The training focused on:

- Understanding time and space as critical risk factors in maritime operations
- Recognising how human behaviour and psychological pressure influence cyber incidents
- Strengthening vendor management, documentation, and access control practices
- Building confidence to respond methodically rather than react impulsively

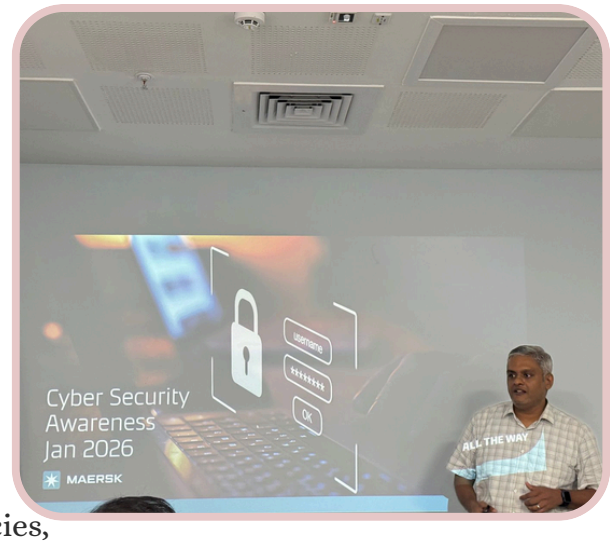
The objective was not fear, but preparedness.

Learning Through Realistic Scenarios

Rather than relying only on theory, the program blended presentations, discussions, and demonstrations with real operational context. Participants examined how cyber incidents unfold onboard, how misinformation can spread during high-stress situations, and how small technical oversights can escalate rapidly.

A key highlight was the live bridge simulation, where scenarios such as GPS spoofing were demonstrated to show how manipulated data can directly affect navigation and situational awareness. This hands-on exposure helped participants connect cyber threats to real-world consequences.

Key Themes from the Sessions



Across the two days, several critical themes emerged:

- The difference between observing and monitoring, and why misinterpreting system behaviour can delay response
- How phishing calls and social engineering are often timed to exploit fatigue during night watches or early mornings
- The risks introduced by IT–OT connectivity and shipside integrators
- Common cyberattack methods such as MITM, DDoS, and ransomware and how they manifest onboard
- Vulnerabilities arising from non-compliance with CSMS policies, including unsecured network switches and unauthorised USB usage

Participants also explored how cyber entry points can exist both onboard vessels and within shore offices, reinforcing the need for a unified approach to cybersecurity.

From Awareness to Action

A strong emphasis was placed on what to do during a cyber incident. Participants were guided through structured response principles designed to reduce confusion and prevent escalation.

Key response practices reinforced included:

- Isolating affected systems promptly
- Avoiding unnecessary reboots
- Preserving evidence through system snapshots
- Informing relevant authorities without delay

The sessions also highlighted the importance of verifying OT system data such as ECDIS, AIS, GPS, and RADAR and recognising signs of manipulation. Practical maintenance measures, including proper cable labelling and system housekeeping, were reinforced as simple yet effective risk-reduction steps.

Strengthening Ship–Shore Alignment

The Chennai training successfully enhanced cybersecurity awareness and operational preparedness by combining technical insight with real-world maritime context. Participants left better equipped to recognise threats early, respond calmly under pressure, and protect vessel safety in an increasingly digital environment. In an industry where seconds matter, preparedness is not optional, it is essential.

Conclusion

One of the most valuable outcomes of the training was improved alignment between shipboard teams and shore-based IT and cybersecurity functions. By developing a shared understanding of risks and response procedures, the program strengthened collaboration, reduced unstructured escalations, and supported faster recovery during incidents. Cyber resilience, the training reinforced, is not the responsibility of one team, it is a shared commitment across ship and shore.

Venue of the Training Centre

Maersk Training India Pvt. Ltd.
Olympia Cyberspace, 4th floor,
21/22, Alandur Road, Arulayiammanpet 2nd street,
Guindy
600032 Chennai
Phone: +919176676885
Direct: +91 8925932144
Mobile: +919176676885
Reg. No. U74210TN2006PTC059795
www.maersktraining.com

List of Attendees

1. **Capt Sounak** -[IT Manager Shoei-Fleet]
2. **Mr Faraz Sayeed** [Ops Manager Shoei IT India]
3. **Mr. Akshay Chavan** [Sr. IT Officer Shoei IT India]
4. **Mr. Roshan Maniyar** [Sr. IT Officer Shoei IT India]
5. **Mr. Sijo Bijomon** [IT Officer Shoei IT India]
6. **Capt Santhosh Kumar Ravi Kumar** [Sailing Staff Shoei-ESM]
7. **2/O - Mr. Saravanan Jagatheesan** [Sailing Staff Wallem Ship Management]

Trainer Details

Capt. Sudhir Kandhari
CEO
Seasoned maritime professional with over 30 years experience. Served as Hydrographic Surveyor Grade I in Indian Navy. 6 years command on Refrigerated Cargo, 11 years on DP2 subsea project vessels.
Rajesh Ganesan
Head of IT operations
20 + yrs in IT Security , Strategy & Infra