FEATURE

THE GROWING ROLE OF CYBERSECURITY AND REGULATORY COMPLIANCE IN THE MARITIME SECTOR

With nearly 90% of the world's goods transported by sea, the maritime sector sits at the core of global trade, economic stability, and safety. The rise of high-bandwidth satellite networks, especially Low Earth Orbit (LEO) constellations, has ushered in unprecedented opportunities for digitisation across vessels and ports. But this increased digital adoption also presents new vulnerabilities. The UAE, whose maritime industry contributed AED 129 billion to its GDP in 2022, is among the nations most committed to strengthening its cybersecurity infrastructure, ranking in the top tier of the 2024 Global Cybersecurity Index. As digital disruption accelerates, cybersecurity is no longer an IT concern—it is a core operational imperative.

THE THREAT LANDSCAPE

Since 2022, there have been at least five major cybersecurity breaches in the maritime sector. Modern maritime operations rely on an intricate blend of onshore IT systems and offshore Operational Technology, including engine control systems,

Jalloul Ben Soussia
Group Chief Technology Officer,
IEC Telecom Group

navigation lights, and automated cargo handling. As these once-isolated environments become integrated, the entry points for cybercriminals multiply. Ships, ports, and cargo terminals are increasingly susceptible to digital sabotage. In the Middle East, the average cost of one cyber breach has soared to $8.75 million, nearly double the global average. Some of the most pressing threats include:

- **Malware and ransomware:** Cybercriminals deploy malicious code to cripple onboard systems, steal data, or demand ransom payments. These attacks can lock out navigation software, access to electronic logs, or crucial safety systems. The Allianz Cyber Center of Competence notes ransomware as the third most-feared threat in maritime in 2023.
- **DDoS attacks:** Overwhelming a ship's systems with traffic can halt operations and impact real-time decision-making.
- **Insider threats and unauthorised access:** Employees with system access, either maliciously or unknowingly, can expose sensitive information, including cargo manifests or crew data.

NAVIGATING EVOLVING COMPLIANCE AND REGULATIONS

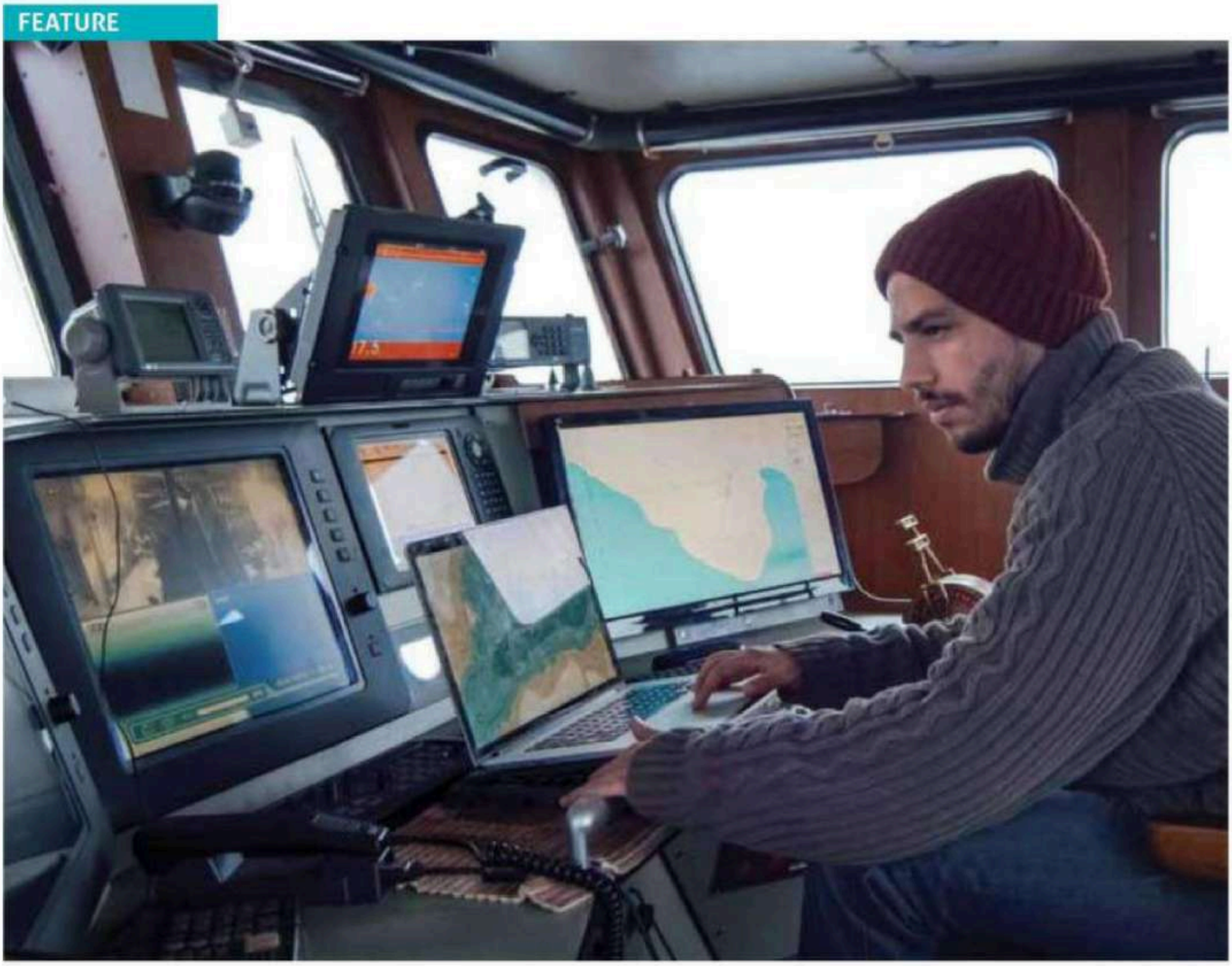
In response to this rising threat environment, the International Maritime Organization (IMO) Resolution 428(98) mandates that shipowners and operators must incorporate cyber risk management into their existing International Safety Management (ISM) Code. Failure to address these risks could render a vessel "unseaworthy" under international conventions, impacting insurance claims and commercial viability. These evolving regulatory demands require flexible cybersecurity frameworks that can dynamically adapt to vessel type, network environment, and threat landscape.

WHAT EFFECTIVE CYBERSECURITY LOOKS LIKE AT SEA

Cybersecurity begins with effective network management. Today, the majority of cyber threats stem from the misuse of personal devices. By segregating crew and corporate networks, vessel operators can significantly reduce the risk of cross-contamination and protect mission-critical systems. IEC Telecom provides advanced network management solutions designed to address this challenge. Managed via the OptiView portal, these systems enable the creation of multiple operational environments on board, supported by a comprehensive analytical dashboard that offers real-time visibility into key performance metrics for each network.

This includes real-time vulnerability monitoring, dynamic filtration controls, and detailed reporting, enabling IT teams to detect threats and enforce policies to mitigate the risks.

No single vessel operates over a single network. As such,



there will always be a backup line for business continuity. While it has a lower bandwidth, this channel is sufficient for remote network maintenance. For instance, IEC Telecom's customer support includes a 24/7 cyber resilience team to run remote troubleshooting and establish policies for automated responses, including the quarantine of suspicious or compromised endpoints to contain incidents and prevent further outbreaks.

THE HUMAN-TECH PARTNERSHIP

Cybersecurity is not a plug-and-play solution. While firewall protection and endpoint antivirus software form a strong perimeter, they are not sufficient in isolation. Organisations must adopt zero-trust security frameworks, which essentially mean that users and devices should not be trusted by default, even if they are connected to a privileged network or have been previously verified. Continuous anti-exploit monitoring is key to success. Systems are now capable of leveraging open-source threat feeds, learning from global incidents, and dynamically updating protocols to protect the on-board network against emerging risks.

That said, any automation still requires human involvement when it comes to management and decision-making. Ultimately, a trained cyber team—either on board or remote—is essential to analyse, adapt, and lead the response to sophisticated, targeted attacks.

CYBER RESILIENCE IS OPERATIONAL RESILIENCE

With the global cost of cybercrime projected to hit $13.28 trillion by 2028, the stakes are too high for reactive approaches. Instead, the industry must embrace a future-ready mindset, one that combines regulatory foresight, technological innovation, and a culture of cyber vigilance. Countries like the UAE are leading the way by investing in smart ports, automated logistics, and national cyber strategies to stay ahead of threats. From shipowners to regulators, the message is that cyber resilience is foundational enabler of maritime trade.

> **“ANY AUTOMATION STILL REQUIRES HUMAN INVOLVEMENT WHEN IT COMES TO MANAGEMENT AND DECISION-MAKING."**