

Cybersecurity at Sea: Building a More Resilient Maritime Workforce Through the CyberSEA Project

By Dr Lakhvir Singh, C4FF

Introduction: Digitalisation and the Growing Cybersecurity Challenge

The maritime industry is undergoing a profound digital transformation. Modern vessels increasingly depend on interconnected operational technology (OT), information technology (IT), satellite communications, electronic navigation systems and digital platforms to support safe, efficient and commercially viable operations. Ports, shipping companies, logistics providers and vessel operators are becoming more connected, enabling greater automation, improved situational awareness and more effective management of global supply chains.

However, this transformation also expands the potential attack surface. Systems that were traditionally isolated are increasingly connected to corporate networks, remote maintenance services and external communication infrastructure. A cyber incident can therefore extend beyond the loss of information or disruption to office-based IT systems. Depending on the systems affected, it could interfere with operational information, communications, machinery monitoring or other functions supporting vessel safety and operational continuity.

Maritime cybersecurity is consequently much more than an IT issue. It is an operational, safety, business-continuity and risk-management concern that requires coordinated action across the maritime workforce.

Addressing this challenge demands more than technical security products. It requires people who understand the maritime operating environment, recognise cyber threats and know how to respond appropriately. This is the context in which the CyberSEA – Increasing Cyber Security at SEA through digital training project is making its contribution.

Co-funded by the European Union through the Erasmus+ programme, CyberSEA focuses on strengthening cybersecurity capabilities in the maritime sector through digital training, practical remote laboratories and educational resources for maritime learners and trainers.

Understanding the Cybersecurity Risks Facing Maritime Operations

Maritime operations depend on a complex combination of digital and physical systems. These include navigation and positioning technologies, electronic chart systems, vessel communications, cargo-management applications, engine and machinery monitoring, and shipboard automation and control systems.

Each system has different security requirements. Conventional IT security often focuses on the confidentiality, integrity and availability of information. Operational technology must also account for physical processes, system availability, operational continuity and human safety.

A compromised business email account, for example, might expose commercial information or facilitate fraudulent payments. A cyber incident affecting operational systems could have different consequences, potentially disrupting access to essential information or affecting the availability of systems supporting vessel operations.

Important maritime cyber risks include:

- **Phishing and social engineering:** Manipulating crew members or shore-based personnel into disclosing credentials, opening malicious attachments or authorising fraudulent transactions.
- **Malware and ransomware:** Disrupting business applications, compromising connected systems or making operational information unavailable.
- **Weak access controls:** Enabling unauthorised access through shared accounts, weak passwords or excessive user privileges.
- **Insecure remote access:** Creating opportunities for attackers to exploit remote maintenance connections, third-party services or poorly secured network access.
- **IT/OT connectivity risks:** Allowing threats originating in business networks to affect operational environments when network segmentation and security controls are inadequate.
- **Navigation-related cyber threats:** Manipulating or disrupting positioning and navigation information, potentially affecting situational awareness and operational decision-making.
- **Supply-chain vulnerabilities:** Introducing risk through software, equipment, contractors, service providers and other external dependencies.

These risks demonstrate why cybersecurity awareness must extend beyond specialist IT departments. Masters, officers, engineers, ratings, shore-based managers, technical personnel and third-party service providers all have a role in protecting maritime operations.

Effective maritime cybersecurity therefore requires a combination of appropriate technology, robust procedures, organisational leadership and competent personnel.

CyberSEA: Connecting Cybersecurity Knowledge with Maritime Practice

A significant challenge in maritime cybersecurity education is translating technical concepts into knowledge that can be applied in real operational environments.

Seafarers work in demanding conditions, often with limited time for additional training. Their cybersecurity responsibilities may differ considerably from those of conventional IT professionals. Training must therefore be relevant to their roles, understandable within the maritime context and sufficiently practical to support sound decisions when cyber risks arise.

CyberSEA addresses this challenge through three principal outputs:

1. A repository of maritime cyber vulnerabilities, supported by relevant scenarios and protocols.
2. An online cybersecurity training course incorporating assessment.
3. Remote laboratories providing practical cybersecurity challenges.

Together, these outputs provide a framework for connecting cybersecurity awareness with structured learning and practical exercises.

The repository supports the identification and understanding of vulnerabilities relevant to the maritime sector. The online course provides a structured learning pathway, while the remote

laboratories enable participants to investigate specific cybersecurity challenges in a controlled environment.

This combination is important. Reading about cyber threats can establish a foundation, but practical exercises help learners understand how vulnerabilities arise, how attacks may unfold and why particular defensive measures matter.

By bringing these elements together, CyberSEA supports the development of cybersecurity knowledge and practical skills within maritime education and training.

From Theory to Practice: Inside the CyberSEA Remote Laboratories

One of the project's most valuable features is its collection of remote cybersecurity laboratories. These provide hands-on exercises designed around different cyber threats and defensive challenges relevant to maritime and organisational security.

The CyberSEA Hub includes laboratories developed by participating partners, covering a range of scenarios.

Phishing detection

Phishing remains a significant risk because attackers frequently exploit human behaviour rather than relying exclusively on technical vulnerabilities. The HMU laboratory challenges participants to identify deceptive emails and develop their ability to recognise phishing attempts.

This type of exercise can reinforce practical skills, including checking sender details, scrutinising suspicious links, recognising unusual requests and following appropriate reporting procedures.

GPS spoofing analysis

Reliable positioning information is important for maritime navigation and situational awareness. The IDEC laboratory focuses on analysing network traffic to investigate a GPS spoofing scenario and identify how the attacker manipulated the relevant protocol.

This exercise illustrates how cybersecurity can intersect with navigation-related risks. It also demonstrates the importance of understanding the integrity and reliability of digital information used in operational decision-making.

Ransomware response

Ransomware can disrupt access to business applications, operational information and supporting services. The Academia Navala laboratory addresses ransomware threats and response planning, helping participants consider how organisations can protect themselves and prepare for recovery.

The broader lesson is that resilience depends not only on preventing an attack but also on having appropriate procedures for reporting, containment, recovery and learning from incidents.

Network security

The SAMK laboratory focuses on network security, unauthorised access and the protection of data transmission. These topics are relevant to understanding access controls, secure configurations and the importance of protecting communication pathways.

Data privacy and social engineering

Other laboratories address sensitive-data protection, privacy and social engineering. These exercises highlight the relationship between technical safeguards and human behaviour, reinforcing the importance of handling information responsibly and recognising attempts to manipulate personnel.

Insider threats

The project also includes laboratories addressing threats originating from within an organisation. Such threats may involve malicious activity, misuse of legitimate access or actions that unintentionally expose systems and information to risk.

These scenarios reinforce the importance of appropriate permissions, monitoring, accountability and a culture in which security concerns can be reported.

Taken together, the laboratories demonstrate the breadth of cybersecurity challenges that maritime professionals may need to understand. They also offer educators practical resources for introducing cybersecurity concepts through activities rather than relying exclusively on lectures and written materials.

The exercises should be understood as controlled training environments, not as substitutes for authorised testing of operational vessels or live maritime infrastructure.

Why Practical Cybersecurity Training Matters for Seafarers

A resilient maritime organisation cannot rely exclusively on a small team of cybersecurity specialists. Its security posture is influenced by the everyday decisions and actions of personnel throughout the organisation.

For seafarers, this may involve recognising suspicious messages, protecting authentication credentials, following approved procedures for removable media, reporting unusual system behaviour and understanding when an incident must be escalated.

For engineering and technical personnel, relevant competencies may include understanding the cybersecurity implications of equipment maintenance, software updates, remote support and connections between operational systems and external networks.

For shore-based managers, the emphasis may include risk assessment, incident coordination, supplier management, staff development and the integration of cybersecurity into established operational procedures.

CyberSEA's emphasis on digital training and practical exercises provides a way to introduce these issues to different groups of learners.

Its relevance extends beyond raising awareness. Effective training should help participants understand the actions expected of them, recognise the limits of their authority and follow established procedures when a cyber incident occurs.

For example, a seafarer who notices suspicious system behaviour should understand the importance of reporting it promptly and avoiding unauthorised changes that could complicate an investigation or affect operational safety.

Similarly, personnel responsible for technical maintenance should appreciate that connecting equipment to external systems, installing updates or granting remote access can introduce cybersecurity risks if appropriate controls are not followed.

These examples illustrate why maritime cybersecurity training must be connected to professional responsibilities and the operational environment in which personnel work.

Digital Learning and International Collaboration

The maritime workforce is international by nature. Seafarers and maritime professionals work across national boundaries, multinational organisations and different education and training systems.

Cybersecurity training must therefore be accessible, relevant and adaptable to diverse learning environments.

Digital learning can help overcome some of the limitations associated with traditional classroom-only delivery. Online resources can support flexible study, while remote laboratories provide opportunities to undertake practical exercises without requiring every participating institution to establish an equivalent physical laboratory.

For vocational education and training providers, this creates opportunities to incorporate cybersecurity into existing programmes and professional development activities.

Cybersecurity can be connected with navigation, engineering, vessel operations, safety management and the wider responsibilities of maritime professionals. Rather than treating it exclusively as a specialist IT subject, educators can demonstrate how security decisions influence operational reliability and safety.

International collaboration also helps bring different educational and technical perspectives into the development of training resources. The CyberSEA Hub illustrates this collaborative approach through its partner-developed laboratories.

For lasting benefits, however, digital training must remain relevant to the people using it. Learning resources should be reviewed periodically, scenarios updated as threats evolve and assessments used to identify areas requiring further development.

The effectiveness of training should ultimately be judged not only by participation or course completion but also by whether learners can apply their knowledge in appropriate professional contexts.

Cybersecurity as Part of Maritime Safety and Resilience

Maritime cybersecurity should be understood in terms of resilience, not simply prevention.

Even organisations with appropriate safeguards may experience cyber incidents. Effective preparation therefore includes the ability to identify suspicious activity, report incidents promptly, contain their effects, recover essential services and learn from experience.

Cybersecurity arrangements must also be consistent with established safety-management practices. Security controls should be implemented carefully, particularly where changes could affect safety-critical systems or equipment availability.

Training can contribute to resilience by helping personnel recognise warning signs and understand their responsibilities during an incident. It can also reinforce the importance of following approved response procedures rather than taking unauthorised actions that could worsen a technical or operational problem.

Nevertheless, training is only one component of a comprehensive cybersecurity programme. It must complement appropriate technical safeguards, secure network architecture, access management, backup and recovery arrangements, incident-response planning, supplier oversight and organisational governance.

The contribution of CyberSEA lies in strengthening the human and educational dimension of this wider approach. By providing structured digital learning and practical challenges, the project supports efforts to make cybersecurity knowledge more accessible within maritime education and training.

Looking Ahead: Turning Training Resources into Lasting Benefits

The long-term value of cybersecurity training depends on sustained adoption, practical relevance and continued evaluation.

For CyberSEA, important considerations include the continued accessibility of its resources, the integration of training into maritime education and professional development, and the ability of instructors and organisations to adapt learning activities to changing risks.

Evaluation should consider whether learners demonstrate improved understanding, make better security-related decisions and follow appropriate procedures in operational settings. Feedback from cadets, serving seafarers, instructors and maritime employers can help identify gaps and inform future improvements.

Where appropriate, training providers and employers could also examine performance in realistic exercises, the quality of incident reporting and adherence to established security procedures.

Another important consideration is the relationship between cybersecurity education and recognised maritime requirements. Training initiatives should complement applicable international obligations, relevant industry guidance and an organisation's own safety and security-management arrangements. They should not be presented as a substitute for regulatory compliance or specialist technical expertise.

The broader opportunity is to make cybersecurity an integral part of maritime professional development rather than an occasional or isolated training activity.

By supporting collaboration between educational institutions, maritime organisations and cybersecurity specialists, projects such as CyberSEA can contribute to a more informed and security-conscious maritime workforce.

Conclusion

The digitalisation of maritime operations brings significant opportunities, but it also makes cybersecurity an essential component of safe and reliable shipping.

Protecting vessels, cargo, operational systems and supporting infrastructure requires a combination of effective technical controls, sound procedures and a workforce equipped to recognise and respond to cyber risks.

The CyberSEA project addresses an important part of this challenge through its maritime cyber-vulnerability repository, online training course with assessment and remote cybersecurity laboratories. Its practical exercises, covering areas such as phishing, GPS spoofing, ransomware, network security, data privacy, social engineering and insider threats, connect cybersecurity concepts with realistic learning scenarios.

The project's wider value lies in its focus on education, practical skills and the development of cybersecurity capabilities across maritime training environments.

The next step is to ensure that these resources continue to be used, evaluated and incorporated into maritime education and professional development. Through sustained collaboration and practical learning, initiatives such as CyberSEA can help strengthen cybersecurity awareness, support better operational decisions and contribute to a more resilient maritime industry.

Ultimately, maritime cybersecurity is a shared responsibility. Building a safer digital maritime environment requires not only secure systems, but also informed people, effective leadership and a culture in which cybersecurity is recognised as an integral part of professional maritime practice.

About the author

Dr Lakhvir Singh is Research Director at C4FF and a computing lecturer specialising in computer networks and cybersecurity. His work encompasses applied research, cybersecurity, digital technologies and collaborative European projects, including CyberSEA. He is a Chartered Marine Technologist (CMarTech) and Fellow of the Institute of Marine Engineering, Science and Technology (FIMarEST).

Explore CyberSEA

- **Project website:** <https://cybersea-project.eu/>
- **Online training course:** <https://course.cybersea-project.eu/>
- **Remote cybersecurity laboratories:** <https://hub.cybersea-project.hmu.gr/>

Funding acknowledgement and disclaimer: The CyberSEA – Increasing Cyber Security at SEA through digital training project is co-funded by the European Union through the Erasmus+ programme (Project Number 2023-1-ES01-KA220-VET-000159793). The views and opinions expressed are those of the author(s) and do not necessarily reflect those of the European Union or the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union nor SEPIE can be held responsible for them.