

# MARITIME CYBER RISK MANAGEMENT

## COURSE OBJECTIVES

- On completion of the course, the participants will:
- Enhance their awareness of external and internal threats, risks and vulnerabilities relating to security of data and digitally held information in the organisation
  - Understand the significance of cyber security measures at the organisational as well as individual employee level
  - Know about cyber security issues specific to maritime industry and their implications
  - Learn about purpose and scope of standards governing cyber Risk Management
  - Be able to function as a security-conscious individual and also as an active team member in giving full effect to implementation of cyber security measures initiated in one's own organisation

## ABOUT THE COURSE

In today's digitally connected, Internet-driven world, with its increasing vulnerabilities originating from anti-social elements, cyber security has assumed an unprecedented significance and urgency. Maritime industry, which has been a relatively new entrant into the digital world has begun to grasp the significance of cyber security- at the organisational as well as employee level.

This course aims to enhance the awareness of participants in respect of the emerging digital security concerns in the maritime industry. It also updates their understanding of the measures initiated and standards developed and applied to ensure effective Cyber Risk Management.

## PARTICIPANTS

Officers and staff of shipping and ship management companies, ports and terminals, shipping agents, suppliers and service providers to the maritime industry.

## DURATION

Half-day

## KEY TOPICS

- External and internal threats, risks and vulnerabilities relating to security of data and digitally held information in the organisation
- Cyber security issues specific to maritime industry and their implications
- Purpose and scope of IMO's 'Interim Guidelines on Maritime Cyber Risk Management' MSC Circular 1526
- How to function as a security-conscious individual and also be an active team member in implementing cyber security measures initiated in one's own organisation?