CYBER SECURITY AWARENESS

A comprehensive program, designed for Modern Shipping

REGISTER NOW

CYBER OUTLOOK

IN SHIPPING

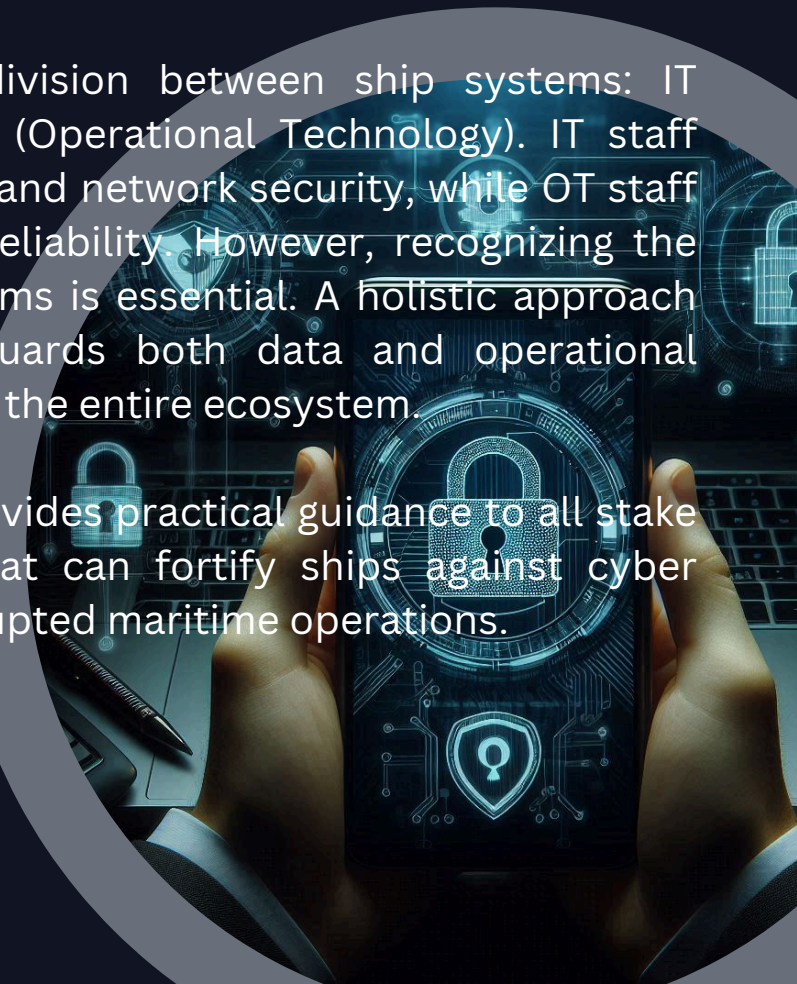
Over the past two decades, significant strides have been made in shore-based internet connectivity. However, the same progress hasn't always extended to shipboard internet access. Fortunately, the landscape is changing due to the increased availability of affordable VSAT / StarLink / SATCOM communications. As a result, the global fleet is becoming better connected.

In 2015, the Futurenautics Crew Connectivity Survey estimated that internet access was available to ships across various fleet sectors at an average rate of 43%. Fast forward to 2019, and this figure nearly doubled to 82%, with a continuing upward trend.

Yet, this newfound connectivity brings with it a heightened risk of cyber incidents. Onboard computers—often outdated—are interconnected without robust security protocols. Cybersecurity procedures and crew training specifically tailored for this environment are frequently lacking.

A critical consideration is the division between ship systems: IT (Information Technology) and OT (Operational Technology). IT staff typically prioritize data protection and network security, while OT staff focus on safety and operational reliability. However, recognizing the interconnectedness of these systems is essential. A holistic approach to cybersecurity—one that safeguards both data and operational continuity—is crucial for protecting the entire ecosystem.

This exclusive training program provides practical guidance to all stake holders, on security measures that can fortify ships against cyber threats, ensuring safe and uninterrupted maritime operations.



RANSOM WARE ATTACKS

STATISTICS 2017 TO 2023

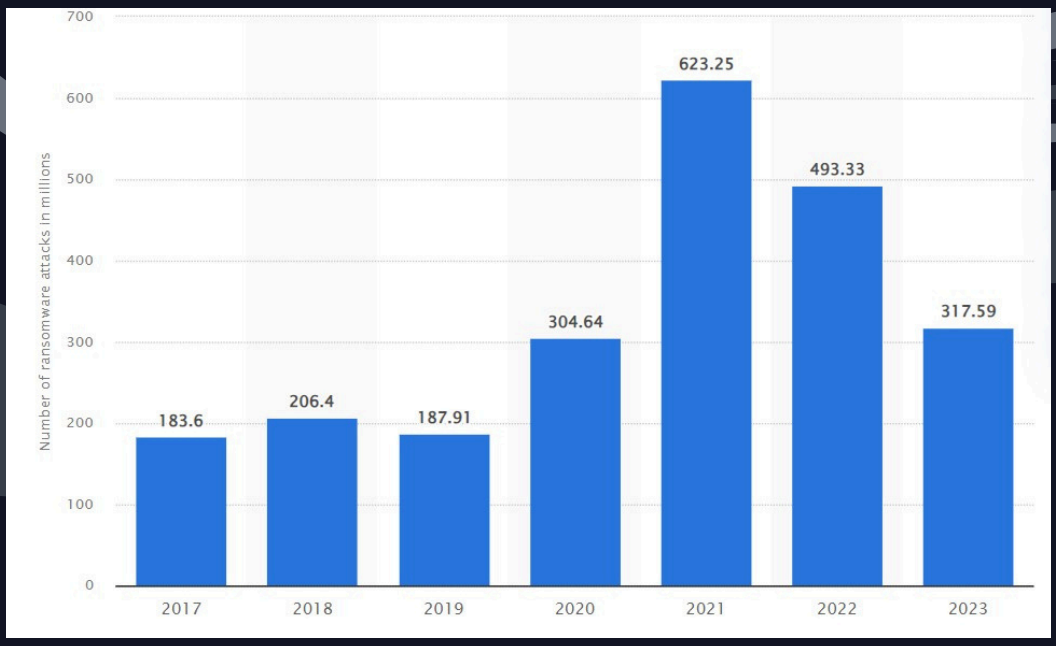


FIG: Annual number of ransomware attempts worldwide from 2017 to 2023 (in million)

In 2022, organizations worldwide detected a staggering 317.59 million ransomware attempts. Interestingly, this number exhibited a significant decline between the third and fourth quarters of 2023—dropping from approximately 155 million to nearly 102 million cases.

Ransomware attacks typically zero in an organization that handle substantial data volumes and play critical roles. When faced with an attack, these organizations often face a difficult decision: pay the ransom to regain access to stolen data or immediately report the incident. Unfortunately, the fear of reputational damage often leads to underreporting of such attacks.

CURRICULAM

SESSION – 1
INTRODUCTION

- What is Cybersecurity?
- Goals of Cybersecurity
- Confidentiality
- Integrity
- Availability
- Components of Cybersecurity
- Information Security
- Application Security
- Network Security
- End-User Security
- Operational Security
- Disaster Recovery Planning
- Cybercrime Statistics
- Introduction to Cyber Attack
- Why do Cyber Attacks happen?
- Who is behind Cyber Attacks?
- What do Cyber Attackers target?
- Business Impact of Cyber Attack
- Case Studies

SESSION – 2
CYBER THREATS & ATTACKS

- Types of Attacks or Threats
- Phishing Attacks & Spam
- Malware
- Password Attack
- SQL Injection Attack
- DoS & DDoS Attack
- Man-in-the-Middle Attack
- Man-in-the-Browser Attack
- Spyware
- Social Engineering
- Ransomware Attacks
- Trojan Horses
- Cryptojacking
- Malvertising Attacks
- Adware

SESSION – 3
PREVENTION OF CYBER ATTACKS

- How Can Employees Help in Improving Cyber Security.
- How to protect from Cyber Attacks?
- Cybersecurity Policies
- Organization Policy for Cybersecurity
- Incident Response Plan
- Cybersecurity Dos & Don’ts

METHODOLOGY

Industry specific training need assessment

Follow Adult Learing Techniques

Identificaiton of Training Needs

Develop and Design specific content

Online Training Session

Evaluate the training

Become Cyber Safe Seafarer

CYBER SECURITY - *A Breach alone is not a disaster, but mishandling is.*

- Serene Davis

In our interconnected world, we all play a role in securing ***CYBER SPACE****.*

- Newton Lee

CYBER INCIDENCE - Reputation takes decades to construct, seconds to shatter

- Stephane Nappo

CONTACT US

KENTER MARITIME CONSULTANCY LLP.

INFO@KENTERMARITIME.COM

+91 89574 82909

WWW.KENTERMARITIME.COM