CYBER ATTACKS

SHIPUNIVERSE

TOP 12 WEAKPOINTS

□ **ECDIS Vulnerabilities**

Problem: Many ECDIS systems are outdated, poorly patched, or exposed via unmonitored network ports.

Risk Mitigation: Regularly update ECDIS firmware, restrict network access, and conduct audits to ensure system integrity.

□ **AIS Spoofing and Manipulation**

Problem: AIS signals can be faked or manipulated to hide vessels, create ghost ships, or mislead navigation systems.

Risk Mitigation: Cross-reference AIS data with radar and other sources; install spoofing detection tools onboard.

□ **Compromised Satcom Systems**

Problem: Satellite communication channels can be intercepted, jammed, or used as access points into onboard networks.

Risk Mitigation: Use encrypted satcom services, apply multi-factor authentication, and limit remote access points.

□ **Crew Devices (USBs, Laptops, Phones)**

Problem: Personal devices can introduce malware to bridge or engine control networks via USB or Wi-Fi.

Risk Mitigation: Disable USB ports where not required, run malware scans on all external devices, and enforce BYOD policies.

□ **Unsecured Remote Access and VPNs**

Problem: Weak remote access controls allow hackers to access ship systems from shore or satellite.

Risk Mitigation: Implement firewalls, require secure VPNs with 2FA, and limit remote access to essential systems only.

□ **Outdated Software and Operating Systems**

Problem: Old software contains known vulnerabilities that are easy to exploit if not patched.

Risk Mitigation: Maintain a software patching schedule and verify with vendors that all critical systems are updated.

□ **Weak or Default Passwords**

Problem: Many systems still run on default admin passwords, offering easy entry for attackers.

Risk Mitigation: Enforce strong password policies, disable default credentials, and rotate passwords regularly.

□ **Poor Network Segmentation (IT/OT Overlap)**

Problem: When navigation, engine control (OT), and crew Wi-Fi (IT) are on the same network, a breach in one affects all.

Risk Mitigation: Create physical or virtual separation between IT and OT systems, with controlled access points.

□ **Phishing Attacks on Crew and Staff**

Problem: Hackers target crew with fake emails to steal credentials or deploy malware.

Risk Mitigation: Train crew to spot phishing attempts, and simulate campaigns as part of ongoing awareness programs.

□ **Insecure IoT Devices and Sensors**

Problem: Sensors added to engines, cargo, or navigation systems may be insecure and go unmonitored.

Risk Mitigation: Only install verified IoT devices, regularly update firmware, and isolate devices on their own VLANs.

□ **No Real-Time Threat Monitoring**

Problem: Without detection tools, attacks may go unnoticed until damage is done.

Risk Mitigation: Use onboard intrusion detection systems (IDS), and integrate with shore-based security operations if possible.

□ **Lack of Crew Cyber Awareness**

Problem: Even basic safety practices aren’t always followed—especially under pressure.

Risk Mitigation: Conduct regular cyber drills and make cybersecurity part of onboard safety training.