• Cyber expertise
• Assessments
• Cyber Threat Intelligence
• Training
• Software
• Cyber risk transfer
Section 1.2.2.2 of the International Safety Management (ISM) Code states:

“Assess all identified risk to its ships, personnel and the environment and establish appropriate safe guards.”
Chapter 6 – Establish Contingency Plans

• “There may be occasions when responding to a cyber incident may be beyond the competencies on board or at head office due to the complexity or severity of such incidents. In these cases, external expert assistance may be required (for example, post event forensic analysis and clean-up).”
Why Discuss Cyber Risk?

Industry Guidelines, BIMCO

BIMCO

The Guideline on Cyber Security onboard Ships

BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL

Chapter 7, Respond to and recover from cyber incidents

– Establish Team: “A team, which may include a combination of onboard and shore-based personnel and/or external experts, should be established to take the appropriate action…….” to restore the IT and/or OT systems so that the ship can resume normal operations.

– Capabilities of Team: “The team should be capable of performing all aspects of the response.”

– Identify Team in Plan: “Details of where this assistance is available and by whom, should be part of the recovery plan,”
Why Discuss Cyber Risk?

Present USCG Regulatory Requirements

US Coast Guard Policy Letter 08-16 of 14 December 2016 – ISPS and MTSA

- Report Suspicious activity
- Report Breach of Security

Report Incidents

- National Response Center
- The National Cybersecurity & Communications Integration Center (NCCIC) – Cyber Incidents
Shipowner’s Recent Email to Hudson after a Significant Cyber Incident:

“It gets even better! Our network is up now but the ERP is still locked down by malware and the entire database appears to be corrupted.

We are now going on three days without (expletive deleted) purchasing, maintenance, personnel/HR, all unavailable.

Best part Mr. X watched our IT manager Googling “how to remove malware” this morning and then downloaded a “free removal tool” from the Internet. Apparently it didn’t work!”
Before a cyber attack occurs:

- **Assess:** Perform a cybersecurity capability assessment of your *entire* organization.
- **Plan:** Establish a cyber *incident response (IR) plan.*
- **Train:** Incorporate cyber risks into tabletop exercises.
- **Integrate Plans:** Data Loss Prevention (DLP), Disaster Recovery (DR) and *Business Continuity Plans (BCP).*

- It’s not *if,* but *when - accept the fact* that your company will one day be breached.
- How your organization responds to the attack and recovers from it is what is critical.
What to Do Now: Preparedness

Ask yourself as an Owner:

• *Who will be there in the middle of the night?* Prepare for the worst – establish cyber incident response capabilities

• *Who will cover our a**?*

• *Who will speak for our company?*

• *Have we appropriately transferred our cyber risk?* Prepare now for cyber insurance (don't assume you have full coverage)
  
  – CL 380 Buyback
  
  – Cyber Liability
  
  – Cyber Incident Response and Recovery
A Cyber Risk Solution Set for Vessel Owners
Cyber QI (CQI) Overview

Shipowner

CQI Contract

Cyber IR Contract

Port State Control
• National:
  • US Coast Guard / Captain of the Port
  • National Response Center
  • NCCIC (CISA)
• State & Local Agencies

Cyber QI (CQI)
• The QI is the contracted owner’s representative
• Contracted Power of Attorney
• Manages all incident response activities
• Administers contracts with all responders
• Provides oversight and approves payments

Operations
Local Port, Marine Terminal and Vessel Liaison / Logistics

Cyber Incident Response Organization (CIRO)
Cyber Technical Incident Response Team (incl. Forensics)

Communications
Strategic Communications
• Internal
• External

Liaison
Legal (Outside Counsel) Support activities provided

Finance
Claims Management and documentation

© 2018 HudsonAnalytix, Inc.
Cyber Incident

Vessel cyber incident

Owner

Cyber QI Hudson
- The QI is the owner’s representative
- Manages all IR activities
- Manages contracts with responders
- Provides oversight / approves payments

Cyber Incident Response Organization (CIRO)
- Cyber Incident Response & Mitigation
- Remote and Onsite support
- Forensics

Fed, State & Local Authorities
Stakeholders, Local Logistics
Legal, Public Relations
Insurance

© 2018 HudsonAnalytix, Inc.
Cyber QI Regime

- **Qualified Individual**
  - Represents Owner in US Jurisdiction
  - Oversees all cyber incident response efforts
  - Liaises with USCG, lawyers, responders, insurers, public, etc.

- **Cyber Incident Mgmt. Team (CIMT)**
  - Cyber IR, forensic specialists/personnel

- **Cyber Incident Resp. Org. (CIRO)**
  - Cyber IR, forensic specialists/personnel

OPA '90 Regime

- **Qualified Individual**
  - Represents Owner in US Jurisdiction
  - Oversees all oil incident response efforts
  - Liaises with USCG, lawyers, responders, insurers, public, etc.

- **Incident Management Team (IMT)**

- **Oil Spill Removal Org. (OSRO)**
  - Spill response experts/personnel
CQI and Process

Hudson Named as Cyber Qualified Individual

Works with/Coordinates:
- USC G
- NRC / CISA
- Outside Counsel
- CIMT
- PR Firms
- P&I Club
- General Public

Proposal → Contract → Questionnaire → Vessel Incident Response Plan Reviewed and Updated

Revised / Approved Incident Response Plan

Coordinate / Align CIRO w/Insurance
Driving Continuous Improvements and Setting the Stage for Long-Term IMO Compliance

Launch HACyberLogix Platform

Allocate Appropriate Resources and Implement Improvements

Prioritize Implementations and Plan Updates to SMS

Perform Baseline Evaluation and Identify Gaps (Workshop)

Review Recommendations, MoC Integration and Set Target Profile

Year one

• Investment Planning
• Resource Allocation
• Mitigation Activities
• MoC and SMS Updates

Year two

• Sustain Investments & Resources
• Mitigation Activities Continue
• Finalize SMS Updates

Year three

Establishing a Sustainable Cyber Risk Management Program

© 2018 HudsonAnalytix, Inc.
Driving Risk Reduction

The Cyber Risk Reduction Curve
Investing in the right combination of technology and insurance maximizes risk reduction.

1. Technology Risk Reduction
2. Insurance Risk Reduction

Courtesy: Axio