Hockey Sticks and Maritime Cyber Security

Marine Insurance Day – October 2, 2020
About us

**Cyber Mariner**
- Independent consultancy – founded 2018
- Acts on behalf of Owners and Operators
- No product sales
- Focus on maritime cyber security / safety

**Cris DeWitt**
- Co-founder of maritime cyber company acquired by ABS in 2012
- First offshore drilling rig cyber assessment
- Co-inventor of FCI Cyber Risk Model
- Founder/Managing Director of Cyber Mariner
- CISSP, GICSP

**Mason DeWitt**
- Maritime Cyber Security Analyst
- Built infrastructure for first purpose-built Formula 1 racetrack
- Maritime Cyber Security Policy/Procedure Expert
RDP to ship Maintenance system from Internet; login to: Ballast control module...

... Make it roll over
3. Market Practices Concerning the Settlement of Claims

240. In addition to the specific contractual provisions of the marine insurance policy and the statutory rules governing such policies, legal regimes governing marine insurance are also composed of informal and often formal rules, customs and practices concerning the transposition of loss of, or damage to, an insured object into a cash indemnity payable to the assured. As a result of the

---

(1) Least Privilege / Authorize Access to Security Functions

The organization explicitly authorizes access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information].

Supplemental Guidance: Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users.
Cyber Security is all About RISK

- Ghost of software
- Integration testing is expensive
- Varying forms of insurance (or exclusions)
- Technology point solutions
- Vulnerabilities outpacing standards
- IT solutions mis-applied to OT
- IT cyber providers that don’t understand safety or maritime
2018 AIMU Cyber Workshop

Practical Cyber Risk Model

**Functions.** Software that control machines on assets

**Connections.** Nature and number of digital interfaces (e.g., physical ports, network connections) indicating cybersecurity complexity

**Identities.** Humans or machines that send or receive data by means of the digital interfaces
All point to some form of risk analysis!
# Cyber Incidents

<table>
<thead>
<tr>
<th>Year</th>
<th>Company</th>
<th>Mode</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>A.P. Moller-Maersk A/S</td>
<td>Malware “drive-by”</td>
<td>cargo booking requests, booking confirmations, booking amendments, bill of lading instructions, cargo tracking, arrival notices, empty container pick up of</td>
</tr>
<tr>
<td>2018</td>
<td>COSCO</td>
<td>Ransomware</td>
<td>failure in its networks, email and phone systems</td>
</tr>
<tr>
<td>2020</td>
<td>Mediterranean Shipping Co.</td>
<td>Malware</td>
<td>myMSC portal network outage, internal data processes</td>
</tr>
<tr>
<td>2020</td>
<td>CMA CGM SA</td>
<td>malware attack based on an engineered targeted vulnerability</td>
<td>ability to communicate with vessels, customers, and marine terminals</td>
</tr>
<tr>
<td>2020</td>
<td>Who’s not talking?</td>
<td>What mode is yet undiscovered?</td>
<td>IT for sure, what about Operational Technology?</td>
</tr>
</tbody>
</table>
The Cyber Divide Between the Boardroom and the Deck Plates
Hockey Sticks and Cyber Security
Cybersecurity Guidance “Burden”

Prescriptive  Outcome

NIST 800-53 Controls  CMMC  Class Societies  NIST CSF Categories  BIMCO  IACS  IMO MSC.428(98)
IMO 2021 Introduction

ISM Code 2018 Edition

1.2.2 Safety management objectives of the company should, inter alia:
.1 provide for safe practices in ship operation and a safe working environment;
.2 assess all identified risks to its ships, personnel and the environment and establish appropriate safeguards; and
.3 continuously improve safety management skills of personnel ashore and aboard ships, including preparing for emergencies related both to safety and environmental protection.

April 7, 2017 – MSC-FAL.1/Circ.3 – Guidelines on maritime cyber risk management

“2.1.4. Effective cyber risk management should consider both kinds (malicious/unintended) of threat.”


“1. „„safety management system should take into account cyber risk management…”

Requirements

- MSC 98/23/Add.1 Annex 10
- MSC-FAL.1/Circ.3 5 July 2017
- DNVGL
NIST Magic Decoder Ring

NIST – Inner 2 rings: 5 Core Functions; 34 Categories
(108 Sub-Categories - not shown)

IMO ISM Code – Outer Ring: 20-25 things
Maritime Cyber Security Considerations

- Cyber Culture (of Owner, Operator, Crew)
- Budgetary constraints and spending plans
- Asset Complexity (age, technical platform)
- Operating Environment (Inland, Offshore…)
- Mission (Cargo type, equipment function…)
- Control Implementation Timing (yard vs underway)
- Route connectivity (LTE, WiFi, Fleet Broadband, VSAT…)

AIMU/IUMI and Cyber Mariner - All Rights Reserved
Illustrations - Damen Shipyards Group © 2020
A Question for Everyone

Why do we push cyber risk to the most expensive and least effective end of the supply chain (post commissioning)?
Supply Chain Considerations

How Iran's Shahid Rajaee seaport was cyber-attacked

Over the past week, as tensions in the Persian Gulf increased between the United States and Iranian forces, Iran reported that its seaports in the region of Bandar Abbas came under a cyber-attack, which caused the Shahid Rajaee port to be shut down for several days. Later reports in the United States attributed the attack to Israel.

It was a series of several cyberattacks that began early this year and culminated in the latest assault.

The cyberattacks on the Iranian port is not the first of its kind and will probably not be the last. A cyberattack on a port and the ability to disable or disrupt port activity is not complicated.

How is a cyberattack on a port carried out, and how can a port be disrupted for days?

Iran's Terminal Operating System

Seaports operate many computerized systems for port management, loading and unloading of containers and cargo from vessels, shipping and storage at the port, customs payments, maritime control and control systems, customer relationship data systems, physical security systems, and more.
Steal This Checklist

✓ Governance
  ✓ Steering Committee
  ✓ Policies / Procedures
  Is someone responsible for cyber security?
  Are cyber activities documented?

✓ Training
  ✓ Awareness
  ✓ Specific Roles
  Are the company, crew, and suppliers aware of cyber practices?
  Do specific roles onboard have specialized cyber training?

✓ Risk Assessment
  ✓ Practical / High-Level
  Has a cyber risk-assessment been performed against critical systems?

✓ Architecture
  ✓ One page, one-line
  ✓ Detailed
  Does a high-level picture of critical systems and connections exist?
  Can a Mariner quickly locate up-to-date system architecture drawings?

✓ Incident Response
  ✓ Onboard
  ✓ Ashore
  Is someone onboard assigned to manage a cyber incident response?
  Is there planned shore-side support for a cyber incident?

✓ Change Management
  ✓ Software/firmware
  ✓ Connections
  ✓ People
  Does a current software/hardware inventory of critical equipment exist?
  Are system connections managed via a robust process?
  Does the Crew follow a change management process for software?
Resources

• Industry Guidance
  • IMO MSC(98)428, MSC Fal.1/Circ.3
  • BIMCO, The Guidelines on Cyber Security Onboard Ships
  • DCSA, Implementation Guide for Cyber Security on Vessels v1.0

• Classification Society Guidance
  • DNVGL Recommended Practice 0496
  • DNVGL Type Approval, Cyber security capabilities of control system components
  • ABS The Application of Cybersecurity Principles to Marine and Offshore Operations, CyberSafety Volume 1, 2
  • ClassNK, ClassIR, Bureau Veritas…

• Awareness Training

cris@cybermariner.com
mason@cybermariner.com
Some definitions

**Maritime safety** is concerned with the protection of life and property through regulation, management and technology development of all forms of waterborne transportation.

**Cyber risk quantification** is the process of evaluating the cyber risks that have been identified and then validating, measuring and analyzing the available cyber data using mathematical modeling techniques to accurately represent the organization's cybersecurity environment in a manner that can be used to make informed cybersecurity infrastructure investment and risk transfer decisions.

**Cyber-insurance** is a specialty lines insurance product intended to protect businesses, and individuals providing services for such businesses, from risks relating to information technology infrastructure, information privacy, information governance liability, and activities related thereto.