CYBERSECURITY: THE NEW ENIGMA
THE PERSPECTIVE OF A P&I CLUB

Boriana Farrar
Vice President / Counsel (SCB, Inc.)
Business Development Director - Americas

NOVEMBER 13, 2019
IMO has issued MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management.

The guidelines provide high-level recommendations to safeguard shipping from current and emerging cyber threats and vulnerabilities and include functional elements that support effective cyber risk management. The recommendations can be incorporated into existing risk management processes and are complementary to the safety and security management practices already established by IMO.

The Maritime Safety Committee, at its 98th session in June 2017, also adopted Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems. The resolution encourages Flag administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the ISM Code) no later than the first annual verification of the company's Document of Compliance after 1 January 2021.
• IMO guidelines presented functional elements supporting cyber risk management.

• Identify: To define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.

• Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.

• Detect: Develop and implement activities necessary to detect a cyber-event in a timely manner.

• Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.

• Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.
THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS

• Produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF, IUMI and World Shipping Counsel

• Updated in 2018
Cyber security approach

- **Identify threats**
  Understand the external cyber security threats to the ship.
  Understand the internal cyber security threat posed by inappropriate use and lack of awareness.

- **Identify vulnerabilities**
  Develop inventories of onboard systems with direct and indirect communications links.
  Understand the consequences of a cyber security threat on these systems.
  Understand the capabilities and limitations of existing protection measures.

- **Assess risk exposure**
  Determine the likelihood of vulnerabilities being exploited by external threats.
  Determine the likelihood of vulnerabilities being exploited by inappropriate use.
  Determine the security and safety impact of any individual or combination of vulnerabilities being exploited.

- **Establish contingency plans**
  Develop a response plan to reduce the impact of threats that are realised on the safety and security of the ship.

- **Develop protection and detection measures**
  Reduce the likelihood of vulnerabilities being exploited through protection measures.
  Reduce the potential impact of a vulnerability being exploited.

- **Respond to and recover from cyber security incidents**
  Respond to and recover from cyber security incidents that are realised using the response plan.
  Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.
IMO – MSC/FAL Circ. 3 (May 2016)

Guidelines on Maritime Cyber Risk Management (previously MSC. Circ 1526)

- Establishes high-level guidelines for a holistic, risk management approach to cyber
- Aligns with NIST Cybersecurity Framework

IMO – Maritime Safety Committee Resolution 428(98) (June 2017)

- Affirms that approved Safety Management Systems should take cyber risk management into account
- Encourages administrations to ensure that cyber risks are appropriately addressed in safety management systems by 1 January 2021

Flag State Implementation (June 2017 – January 2021)

- USCG collaborating with industry to develop a clear path to compliance with MSC Resolution 428(98)
- Development of industry standards, Company implementation, verification, and feedback through the SMS audit process
USCG MARINE SAFETY ALERT: CYBERSECURITY

• The US Coast Guard (USCG) has issued a Marine Safety Alert 06-19: *Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels*

• All vessel and facility owners and operators should conduct cybersecurity assessments to better understand the extent of their cyber vulnerabilities:
  • Segment networks
  • Per-user profiles & passwords
  • Be wary of external media
  • Install basic antivirus software
  • Don’t forget to patch

• Marine Safety Information Bulletin (MSIB) 04-19
• ICS Alerts
• ICS Advisors
• ICS-CERT Monitor Newsletter
• https://www.us-cert.gov/security-publications
• IG P&I policies do not specifically identify cyber risks
• A cyber ‘hostile act’ or act of terrorism (a war risk) would be excluded from P&I cover
• FD&D Cover - may be coverage for legal costs & guidance if crime/dispute/loss directly involves an insured vessel
Scenario 1

- Unauthorized access into an agent’s email system
- Impersonation of the agent
- Funds directed to impersonator’s bank account
- Fraud
- Own economic loss falls outside standard P&I cover
- FD&D
- Learn to spot the red flags
Scenario 2

- Malware is installed by seafarer’s mistake (e.g. infected USB stick) interferes with its navigation systems and leads to collision, injury, death etc.
- P&I would respond in the normal course
- Training & policies = lead to prevention
Scenario 3

- Compromised monitoring system (known terrorist acknowledges responsibility)
- Falls into war & terrorism exclusion
- Training and policies mitigate risk
Additional Maritime ‘Cyber’ Legislation Involving Shoreline Operations

• ISO / IEC 27000 series of standards and guidelines cover shoreside operations, not shipboard

• International Ship and Port Facility Security Code (ISPS) Code related to the risk of the ship / port interface
The US Coast Guard (USCG) has issued a Marine Safety Alert (MSA) Cyber-Imperative: Critical Deterrents: Vulnerability and Commercially Oriented Cyber Threats, prompted by a recent electronic threat that targeted a specific vessel. Significantly, since 2016, the USCG and American Club have issued numerous alerts to address cybersecurity risks.

In closing statements from its investigation, the USCG noted that these reports set forth the latest and important findings of on-going investigations. The USCG is committed to continuing efforts to ensure industry-wide awareness and implementation of various security measures. These findings are critical to mitigating the effects of non-compliance and vulnerabilities.

The MSA is intended to ensure that vessels are prepared for the potential threats. To enhance awareness and readiness for responding to threats, USCG is urging all marine operators to take necessary actions to protect their interests. The USCG encourages all stakeholders to work together to mitigate the risk and enhance cybersecurity practices.

Member Alert - USCG MARINE SAFETY ALERT: CYBERSECURITY issued 7/2019

Member Alert - American Club Cyber Security Guidance issued 2/2016:

Questions?
Thank You!

The American Club

1914