Development of cyber security guidelines for the shipping industry

DIRK FRY – COLUMBIA SHIP MANAGEMENT
CHAIR OF BIMCO MARITIME SECURITY COMMITTEE
Today’s Cyber presentation

- Background to the development of industry cyber guidance
- The guidance - understanding the risks on board ships and their vulnerabilities
- What can we do to reduce the risk?
Agility needed

• Cyber attack techniques develop constantly – it is a dynamic threat - so mitigating measures will also have to change constantly.

• Processes and procedures are needed to address

• IMO regulation would be too slow to implement and indeed then change.

• Type approval of software is not the full answer, as it is a static process

• We see an industry best management practice as the way to operationally cope with cyber security
The Stakeholder Decision – Who to Address

Guidance could not address all industry stakeholders – just the bottom line

Indeed, guidance is not even sector specific but addresses shipping as a whole
IMO process however has started

• At IMO MSC 94 (June 2015) Paper promised by BIMCO, ICS, INTERTANKO and INTERCARGO to submitted to MSC 95

• BIMCO, CLIA, ICS, INTERCARGO and INTERTANKO and others have submitted the Industry Guidelines on Cyber Security on board Ships to the next session of the IMO Facilitation Committee (FAL) as an ‘Inf paper’ in order to inform on the industry view and work.

• The same grouping, with now others, is submitting the guidance paper to the Maritime Safety Committee 96 (MSC) for consideration

• The industry aim is to provide guidance rather than regulation in what is a dynamic and complex subject area
BIMCO’s work

• In March 2014, cyber security added to the agenda of the Marine Committee and the Security Committee

  • Concluded that it was necessary to develop industry guidance solely on cyber security for ships and not the whole maritime sector.

  • Started to research the issues and way to address the problem

• In Spring 2015 the RT (BIMCO, ICS, INTERTANKO, INTERCARGO) agreed to develop the guidance as a joint industry project with a BIMCO lead.

• In December 2015 produced .................
THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS

Produced and supported by BIMCO, CLIA, ICS, INTERCARGO, and INTERTANKO
Defined a Shipboard Cyber Incident

An occurrence that actually or potentially results in adverse consequences to an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences.
Aim and Rational

• The aim of the document is to offer guidance to shipowners and operators on how to assess their operations and put in place the necessary procedures and actions to maintain the security of cyber systems onboard their ships.

• The Guidelines are designed to develop understanding and awareness of key aspects of cyber security. The Guidelines are not intended to provide a basis for auditing or vetting the individual approach to cyber security taken by companies and ships.

• Existing international standards and guidelines cover cyber security issues for shoreside operations – whereas these Guidelines focus on the unique issues facing the shipping industry onboard ships.
The Industry Guidelines on Cyber Security on board Ships

The guidance therefore addresses:

• Understanding the cyber threat
• Assessing the risk
• Reducing the risk
• Developing contingency plans
# Understanding the Cyber Threat to Ships

<table>
<thead>
<tr>
<th>Group</th>
<th>Motivation</th>
<th>Objective</th>
</tr>
</thead>
</table>
| **Activists (including disgruntled employees)** | • Reputational damage  
  • Disruption of operations | • Destruction of data  
  • Publication of sensitive data  
  • Media attention |
| **Criminals**                      | • Financial gain  
  • Commercial espionage  
  • Industrial espionage | • Selling stolen data  
  • Ransoming stolen data  
  • Ransoming system operability  
  • Arranging fraudulent transportation of cargo |
| **Opportunists**                   | • The challenge                  | • Getting through cyber security defences  
  • Financial gain            |
| **States**                         |                                   | • Gaining knowledge  
  • Espionage                           | • Disruption to economies and critical national infrastructure. |
| **State sponsored organisations**  |                                   |                                                   |
| **Terrorists**                     |                                   |                                                   |
Understanding ships are vulnerable to cyber attacks

• Ships are chartered to 3rd party operators
  • The shipowner does not have control over the IT systems required by the charterer
• Passengers and other external persons have access to the ships
• Critical data pertaining to cargo is passed through numerous land-side entities
  • Penetration of the weakest link in the chain can result in any data element being compromised
• A high reliability on IT systems related to safety
  • ECDIS and satellite receivers make a ship susceptible to either penetration or jamming
Assessing the risk
A risk based approach

• Some organisations, ships and systems may be more at risk than others, depending on the type and value of data stored
• To manage risks, ships’ personnel and owners should know and understand the probability of an event occurring and the resulting impact.
Assessing the Risk
Some typical risks on board ships

- Remote attacks by criminals
- Insiders introducing malware by storage devices etc.
- Lack of access-control for computers and networks
- Outdated software
- Unprotected or badly designed hardware and networks
- Lack of software and system monitoring
- Insiders introducing malware by storage devices etc.
The Risk Process

- **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 on board systems with direct and indirect communications links.
  - Understand the consequences of a cyber security threat on these systems (including safety).
  - 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 exposed by inappropriate use.
  - Determine the security and safety impact of any individual or combination of vulnerabilities being exploited.

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

- **Respond to Cyber Security Incidents**
  - Respond to cyber security threats that are realised using the Response Plan.
  - Assess the impact of the effectiveness of the Response Plan and re-assess threats and vulnerabilities.
Reducing the Risk
Technical and Cyber Security Controls

Controls to be considered:

- Limitation to and control of network ports, protocols and services
- Configuration of network devices such as firewalls, routers and switches
- Secure configuration for hardware and software
- Email and web browser protection
- Satellite and radio communication
- Malware defences - scanning software will be able to be updated.
- Data recovery capability
- Wireless access control
- Application software security (patch management)
- Secure network design
- Physical security
- Boundary defence
Reducing the Risk
Procedural Controls

Procedural Controls to be considered:

• Training and awareness
• Upgrades and software maintenance
• Anti-virus and anti-malware tool updates
• Use of administrator privileges
• Operations and often full access to systems.
• Physical and removable media controls
• Equipment disposal, including data destruction
Reducing the Risk – Defence in Depth

- The complexity and potential persistence of cyber threats means that a defence in depth approach should be considered.

- Equipment and data protected by layers of defences are more resilient to cyber attacks than equipment and data protected by only a single layer of defence.

- Effective defence in depth may include:
  - multiple layers of technical measures combined with robust policies,
  - security procedures and access controls.

- Existing security measures preventing access to the ship may be considered as a layer within the defence in depth. E.g. Preventing unauthorised access to the ship and ship systems has a role in ensuring that cyber vulnerabilities are not introduced or exploited.

- Company policies should align cyber security with the requirements in the ISM and ISPS Codes and appropriately include relevant procedures.
Contingency Planning

• Ship and Company response plan - covering:
  • Communications
  • Analysis
  • Mitigations

• Recovery Plan – covering
  • Cyber improvements
  • Modifications
  • Corporate communications/damage control

• Investigation of Cyber incidents should result in:
  • A better understanding of the threats facing shipping companies and the ships they operate;
  • Identification of lessons learned; and
  • Updates to technical and procedural control measures, as appropriate.
Current Shipboard networks – planning considerations

• General – Common Core Systems
• Communications
• Navigation
• Propulsion
• Access control
• Cargo Control
• Passenger Servicing Systems
• Crew Management Control Systems
• Passenger Facing Networks
Special/Specific Attention

Cyber security should be carefully considered:

• When taking over a new building and buying used tonnage
• In connection with on-board software maintenance
• When dealing with an always open online connection
It starts during construction of a ship

• Producer should have a QA system for software lifecycle activities, which specifies cyber-security considerations

• Ships networks should be configured to have controlled and uncontrolled networks
Summary of Cyber Security Fundamentals

**IDENTIFY THREATS**
- Be aware of commercial sensitive information
- Identify how systems can be compromised by internal and external sources
- Understand how your ship is connected to external networks and computers

**IDENTIFY VULNERABILITIES**
- Identify and register the IT and OT systems on board
- Know the impact of incidents
- Seek robust technical solutions when changing systems

**ASSESS RISK EXPOSURE**
- Identify the level of cyber safety and security risk
- Determine the likelihood of internal and external threats being exploited
- Recognise where to improve existing protection measures

**DEVELOP DETECTION AND PROTECTION MEASURES**
- Do not allow unauthorised computers or removable media to connect
- Keep the shipboard software maintained and up to date
- Manage users and restrict access to sensitive information and computers
- Make a backup of systems relying on stored data
- Train personnel on how to minimize the risk

**ESTABLISH CONTINGENCY PLANS**
- Have a cyber safety and security policy in place to manage risks
- Know who to call for assistance to restore and repair IT and OT systems
- Prepare restoration measures to be used after an incident
- Train personnel to be able to navigate and operate the ship manually

**RESPOND TO CYBER INCIDENTS**
- Inform about incidents
- Learn and improve after an incident
- Take actions to identify the source of intrusion
Summary Observation: Attacking a ship will not stop world trade

• A ship is an independent unit and a cyber attack may compromise safety of that ship, the marine environment and to some extent, the business continuity of the owner

• To a large extent however the crew will use the same contingency plans as for any other safety or security emergency if the ship is compromised
Conclusions

• Greater awareness is needed in the industry
• Ships are exposed to cyber-threats calling for a risk based approach to mitigate in what is a dynamic environment.
• Industry Guidance has been submitted to FAL 40 and to MSC 96.
• Cyber crime is constantly developing and we need to keep up with it.
• In the future Cyber security considerations should start at the software production stage and cyber robustness considerations should be made when the ship is constructed.