Cyber Risks from the Perspective of a Classification Society

CCNR - Workshop on cybersecurity in inland navigation

Svante Einarsson: Team Leader Cyber Security

05 September 2019
Safety in shipping today heavily depends on cyber systems

Information Technology (IT)
- IT networks
- E-mail
- Administration, accounts, crew lists, ...
- Planned Maintenance
- Spares management and requisitioning
- Electronic manuals & certificates
- Permits to work
- Charter party, notice of readiness, bill of lading...

Operation Technology (OT)
- PLCs
- SCADA
- On-board measurement and control
- ECDIS, GPS
- Remote support for engines
- Data loggers
- Engine & Cargo control
- Dynamic positioning, ...

At risk:
- Mainly finance and reputation
- Life, property and environment + all of the above
The cyber threat to ship, its crew and environment

AIS Spoofing

GPS Jamming of Spoofing

ECDIS updating resulting in loss of fuel control & ballast water valves

Hackers took “full control” of navigation systems for 10 h

ECDIS ransomware & chart spoofing

Loss of main switchboard due to ransomware
The cyber threat also includes risks to the enterprise

- Hacking of cargo tracking system for smuggling purposes
- Pirate attack supported by cyber attack
- Finance, payroll, and operations data breach
- Maersk hit by cyber attack on Tuesday 27th June.
- Via an update to an accounting system in Ukraine
- Spread like a worm from an infected machine
- Global network is infected & all company systems down
- Forced to halt operations at 76 port terminals
- Reinstall 4000 servers, 45000 PCs, & 2500 applications
- Impact to earnings: $200 to 300m (mainly Maersk Line)
- NotPetya was not targeted specifically for Maersk
- Vulnerability fix by Microsoft on March 14th (MS17-010)

- Ransom demanded to avoid release of confidential information
- NotPetya cyber attack hits corporate earnings
Cyber security regulations are evolving…
i.e. IMO Resolution MSC.428(98)

- **AFFIRMS** that... **safety management system should take into account cyber risk management** in accordance with the ISM Code.
- Where to start: MSC-FAL.1/Circ.3
  - IT and OT systems
  - Identify – Protect – Detect – Respond – Recover
  - referring to international best practices
- However, not addressing:
  - how to assess the risk,
  - prescriptive or goal-based safety requirements,

**Impact:**
Cyber risks should be addressed in safety management systems no later than the first annual verification of DoC after 1 January 2021. This is a non-mandatory requirement.

**Outcome:**
MSC 98 adopted recommendatory MSC-FAL.1/Circ.3 superseding the interim guidelines.
Flag states requirements are developing

- USCG CG-5P Policy Letter No. 08-16 require incident reporting (Dec 2016)
- The Coast Guard Blog for Maritime Professionals, 2017-06-30: IMO approves resolution on cyber risk management
- BG Verkehr ISM Cyber Security affirms MSC.428(98) (June 2018)
- Danish Maritime Authority - Order no. 46 makes MSC.428(98) and MSC-FAL.1/Circ.3 mandatory (January 2019)
- Norwegian Maritime Authority – News article: Cyber risks in the maritime sector, 2019-08-19, require cyber risk management according to ISM code
- Data Processing and Cybersecurity Notification Obligation Act (Jan 2016)
- Irish Department of Transport, Tourism and Sport affirms MSC.428(98) (March 2018)
- Maritime and port authority of Singapore affirms MSC.428(98) as quickly as possible, no later than 1st of Jan 2021
- Indian Ministry of Shipping – ENGG. Circ. No.06 of 2017 makes MSC.428(98) and MSC-FAL.1/Circ.3 mandatory from 1st of Jan 2021
- Hong Kong Merchant Shipping Information Note No 40/2017 affirms MSC.428(98)
Commercial stakeholder requirements

Releases cyber security clause
(2019-06-04)

The tanker sector leading the way on cyber security

The insurance sector starting to provide cyber cover
...and DNV GL has follow-up with additional support
All Three Pillars of Cyber Security must be addressed

**People**
- Training & Awareness
- Professional skills & qualifications
- Emergency drills
- Authorizations & authentication
- Physical Security

**Technology**
- System design
- Hardening of connections
- Software configuration
- Encryption protocols
- Jamming & spoofing
- Detection & monitoring

**Process**
- Management Systems
- Governance Frameworks
- Policies & procedures
- Vendor/Third party contracts-follow up
- Audit regimes
DNV GL Cyber Security ISM audit checklist (to be released in fall of 2019)

- Check list elements:
  1. Leadership and commitment
  2. Identify
  3. Protect
  4. Detect
  5. Respond
  6. Recover
  7. Continuous improvement
- ~ 25 areas
- ~ 75 topics

<table>
<thead>
<tr>
<th>Area Name</th>
<th>Checklist question</th>
<th>Examples of evidence</th>
<th>ISM code ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ELEMENT 1: Leadership and Commitment</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Roles and responsibilities</td>
<td>Are cybersecurity roles and responsibilities for the entire workforce established?</td>
<td>Job descriptions; Org. charts</td>
<td>3.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A 3.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A 3.5.1</td>
</tr>
<tr>
<td>Organizational objectives</td>
<td>Are priorities for organizational mission, cyber security objectives, and activities established?</td>
<td>Safety and environmental protection policy; CS Policy; MoM Management Review</td>
<td>1.2.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A 3.5.1</td>
</tr>
<tr>
<td>Legal and regulatory requirements</td>
<td>Are legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, understood and managed?</td>
<td>Safety and environmental protection policy; CS Policy; Legal Register</td>
<td>1.2.3.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>10.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A 4.1</td>
</tr>
<tr>
<td>Management commitment</td>
<td>Do the senior executives understand their roles &amp; responsibilities for cybersecurity?</td>
<td>CS Policy; Interviews</td>
<td>3.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A 3.3</td>
</tr>
</tbody>
</table>

Benefit: providing concrete requirements to uniformly check cyber security resilience and compliance with the IMO Resolution MSC.428(98) and the ISM Code
Examples of findings

- Unsafe behaviour
- Disaster recovery scenarios do not include cyber attacks
- Firewall mounted in engine performance monitoring cabinet, but not connected
DNV GL Cyber Secure class notation

Cyber Secure (Basic)

Target: Operational vessels
Security: Level 1 *(Marinized IEC 62443-3-3)*
Protection: Minimum
Rationale: Security via people, processes & existing systems (technology)

Cyber Secure (Advanced)

Target: New building vessels
Security: Level 3 *(Marinized IEC 62443-3-3)*
Protection: Higher
Rationale: Security via people, processes & integration of systems into the design

Cyber Secure (+)

Target: Operational & new building vessels
Security: defined by risk assessment
Protection: defined by risk assessment
Rationale: Security of additional target system(s) based on client needs

Can be combined with Basic and Advanced

<table>
<thead>
<tr>
<th>SL1</th>
<th>SL2</th>
<th>SL3</th>
<th>SL4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection against casual or coincidental violation</td>
<td>Protection against intentional violation using simple means, low resources, generic skills, low motivation</td>
<td>Protection against intentional violation using sophisticated means, moderate resources, OT system specific skills, moderate motivation</td>
<td>Protection against intentional violation using sophisticated means, extended resources, OT system specific skills, high motivation</td>
</tr>
</tbody>
</table>

Rules are based on IEC 62443 series
How to manage your cyber risks

**Plan**
- ✓ Identify vessel cyber security objectives
- ✓ Make an inventory of systems & software
- ✓ Execute cyber risk assessment & tests

**Do**
- ✓ Establish cyber security policy & procedures
- ✓ Define responsibilities and tasks
- ✓ Execute cyber security training
- ✓ Segregate network & harden devices
- ✓ Report cyber events & incidents

**Act**
- ✓ Execute corrective & preventive actions
- ✓ Obtain verification of effective cyber security
- ✓ Strive for continuous improvement

**Check**
- ✓ Evaluate effectiveness of reaching objectives
- ✓ Analyse cyber incident & event reports
- ✓ Execute internal audits of cyber security
Thank you for your attention!

For further information please contact:

Svante Einarsson
Team Leader Cyber Security

Svante.einarsson@dnvgl.com

www.dnvgl.com