Investing in Cyber Security -
Ensuring Operational Safety & Efficiency

6th Annual Capital Link Maritime CSR Forum - London, 2\textsuperscript{nd} November 2016

KNUT ORDING, PROGRAMME MANAGER DNV GL, DSI - CYBER PHYSICAL SYSTEMS
Agenda

- Cyber security trends
- Industry response
- Cyber security - how it works
- Recommendations
Cyber security trends
Why should we care?
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
- Electronic 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
Cyber security issues are present and migrating to the OT world

Source: AV-TEST Institute, Germany

Source (report extract): “SCADA safety in numbers” – Positive Technologies – October 2012

OT: Operational Technology such as Industrial Control Systems, SCADA, PLCs, Sensors
SCADA: Supervisory Control and Data Acquisition (Operator control and monitoring systems)
Industry response

How has the industry reacted?
Industry response: Cyber Security guidance

RECOMMENDED PRACTICE

Cyber security resilience management for ships and mobile offshore units in operation

*IMO

*ISO/IEC 27001

*IT + OT

*BIMCO: Baltic and International Maritime Council

What

How?
**ASSESSMENT**

- **High-level assessment:** identification of key risks
- **Focused assessment:** barrier management methodology applied to specific high-risk systems
- **In-depth assessment:** comprehensive risk assessment, comparison of current safeguards with target

**IMPROVEMENT**

- **Competence & awareness building**
- **Technical measures:** e.g., access control, software configuration management and barrier management
- **Information security management system (ISMS)**: preparation of documentation and implementation

**VERIFICATION**

- **Monitoring and testing** of technical barriers
- **Verification of ISMS** - against ISO/IEC 27001
Cyber security resilience management
How does it work?
First: Understanding cyber attack mechanics: Attacker → Vulnerabilities → Barriers → Consequences

- **Attack threats**
- **Attack techniques**
- **Vulnerabilities**
- **Security barriers**

**Attack**
- USB port handling
- Default passwords
- Outdated software
- Unsecure Remote connection

**Barriers**
- ECDIS
- CMS
- RADAR

**Consequences**
- Cargo hijacking
- Extortion
- Collision
Focused assessment
**Comprehensive, in depth assessment**

1. Identify critical systems
2. Determine Consequence
3. Determine Likelihood
4. Determine cyber security risks
5. Compare current safeguards with target

**System type**

- **IT**
- **OT**

**Establish prioritised action plan**

- **Likelihood**
  - Medium
  - High
  - High

- **Consequence**
  - Low
  - Medium
  - High
  - Low
  - Low
  - Medium
Improvements

Cyber Security Improvement Roll-out

- Situation Awareness
- Competence Building
- Solidification
- Updated Policy & Procedures
- Predictive & Proactive

Reactive

Cyber Security Maturity
Summary and Recommendations
Where to start?
Digital vulnerabilities in the Maritime sector

DNV GL assessment for Norwegian Authorities*/ Lysneutvalget, April 2015  *Ministry of Justice and Public Security

Top 10:

1) Lack of attention and training
2) Navigation Signals from a satellite is normally not protected against modification
3) Systems for identification of the vessel is normally not protected against modification
4) Remote Maintenance
5) A large number of parties are exchanging a lot of information on unsecured email
6) Separation of computer networks
7) Use of mobile storage devices
8) Booking systems and administration systems are vulnerable
9) Lack of physical security for server rooms, wiring closets, etc.
10) Limited user authentication against systems for public reporting

Participants:
Ship-owners, Authorities (Sjøfartsdirektorat, Kystverket), Interests Organizations (Ship-owners' Association, Norwegian port Association), Insurance (DNK), Supplier (Kongsberg Maritime), Lysneutvalget, DNV GL
Assessment is key: Before spending money on a cyber security initiative, we recommend to carry out a structured and targeted assessment of the risk picture.

**ASSESSMENT**
- Self-assessment app in My DNV GL
- Cyber security assessment

**IMPROVEMENT**
- eLearnings
- Preparation for ISMS certification (27001)
- Consulting on cyber security enhancement

**VERIFICATION**
- Penetration testing
- ISO/IEC 27001
Thank you for your attention!

Learn more, download the RP free of charge and get access to our Cyber Security services from:

www.dnvgl.com/cs

DNV GL Maritime
cybersecurity.maritime@dnvgl.com
Knut.Svein.Ording@dnvgl.com

www.dnvgl.com

SAFER, SMARTER, GREENER