



MINISTRY OF ENVIRONMENT,
ENERGY AND THE SEA

Directorate-General for Infrastructure,
Transport and the sea

Maritime Affairs Directorate

- CYBER SECURITY - reinforcing the level of the ship

Tell me more :
www.ssi.gouv.fr

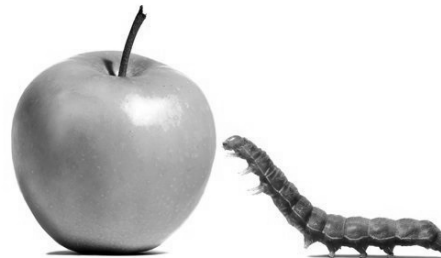


Goal :

*Make ship's owner aware of
cyber risks.*

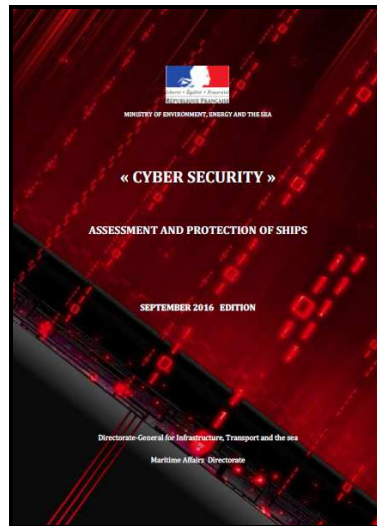
Vulnerabilities ...

- The vulnerability of information and operational ship's equipment systems and the dependence of the ship on these systems,
- The interconnectivity of information systems on and off the ship,
- The development of Internet Of Things (IOT), smartphones or tablet...
- The failure to implement an information or operational technologies security plan and contingency plan on board the ship,
- Lack of crew training to assess malicious acts.



... Risks.

- A breach of the company's image may lead to a loss of competitiveness of the company,
- The sabotage of the ship by a dormant system or operated on demand which can lead to the loss of the ship, the loss of the crew or damage to the environment.



Guideline n°1

(Investigations = 7 guidance cards)

Issue from investigations, this document describes the measures to be implemented in order to raise the level of ship's protection.:

- **R1/** Digital reliability of the ship,
- **R2/** Governance,
- **R3/** Access and data exchange management,
- **R4/** Exchanges security,
- **R5/** Operation continuity,
- **R6/** Traceability and audit,
- **R7/** Confidentiality.

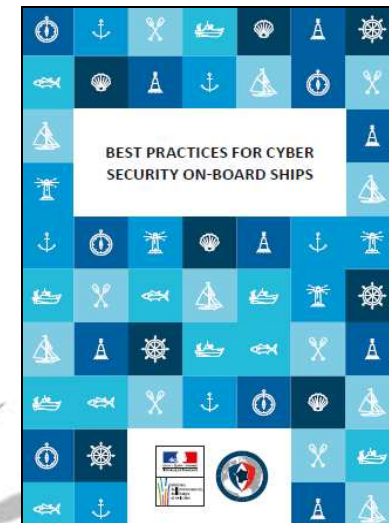


Guideline n°2

(A risk assessment)

This document issue from risk assessment analysis of guidance n°1 describes actions that should be engaged by the company to raise cybersecurity level of ship's Industrial Control System. Three levels meet this demand :

- **L1/** Global security strategie and management of internet of things (IOT),
- **L2/** Passive monitoring,
- **L3/** Hardening configuration of industrial supervision chain systems.



Guideline n°3

(Raise seafarers awareness)

This last guidance aims at raising the awareness of seafarers in order to better understand cyber risk. The actions concern the "hygiene" measures to have :

- Choose strong passwords,
- Use e-mail carefully,
- Separate personal and professional uses,
- Be careful on the Internet,
- Save your data on a regular basis,
- Control installed software on your IT devices...

WEBSITE : <http://www.developpement-durable.gouv.fr/surete-des-navires-et-surete-portuaire>