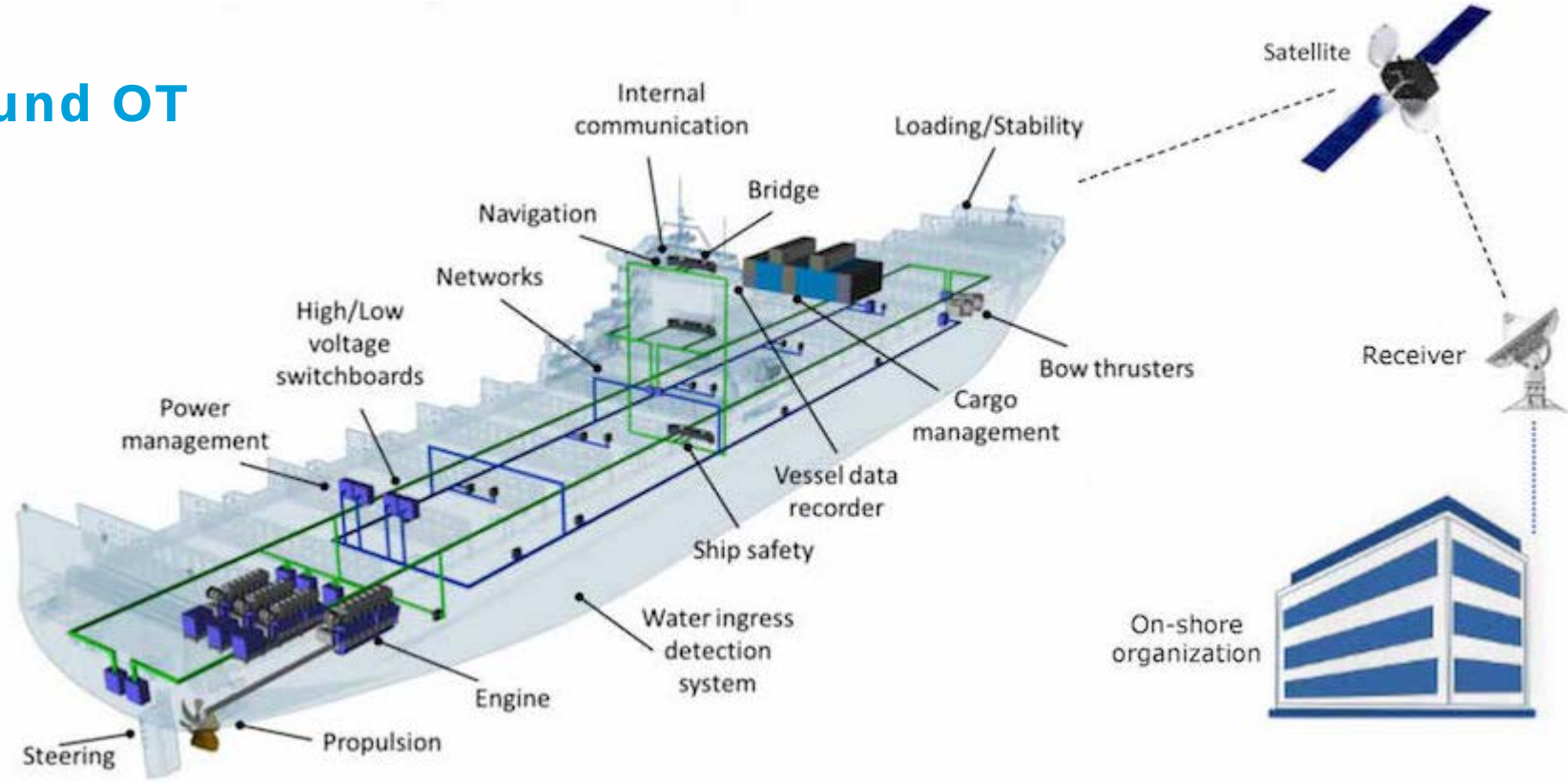
Digitalisierung und ihre Auswirkungen auf das Personalmanagement in der Schiffsbetriebstechnik.

Dr.-Ing. Bettina Kutschera
GL Maritime Software GmbH, Rostock

Schiffsbetriebstechnik: IT und OT

- IT (Information Technology)
  - IT Netzwerk, Email
  - Administration, Crewlisten, Reisepass
  - Wartungsüberwachung
  - Ersatzteilmanagement
  - Elektron. Zertifikate
  - Charterer, Konossement …
- OT (Operation Technology)
  - Supervisory Control and Data Acquisition (SCADA)
  - Mess- und Überwachungssysteme, Fernsteuerung, Daten Logging
  - ECDIS, GPS, AIS, vessel tracking and monitoring systems (VTMS)
  - Dynamic Positioning …



Risiko IT:

- Finanziell
- Reputation

Risiko OT:

- Wie bei IT +
-Personen-, Sach-, Umweltschäden

[Quelle: www.hellenicshippingnews.com]

Trend Cyber-Risiken im Schiffsbetrieb

- Cyber-Bedrohungen Teil des täglichen Geschäfts
- Beispiele von DNV-GL Bord-Inspektionen:
  - Infizierte ECDIS-Karten-Updates bewirken, dass EDCIS-Systeme von 2 Bulkern abgeschaltet werden.
  - Ransomware auf Cpt‘s PC führt zum Verlust der Hauptschalttafel und Stillstand für 3 Tage.
  - E-Mail an Besatzungsmitglied, in der „Manager“ nach Passwort-Bestätigung fragte.

[Quelle: Svante Einarsson, DNV GL]

Auswirkungen – 2 Beispiele

MAERSK LINE

We are sorry but maerskline.com is temporarily unavailable

We confirm that some Maersk IT systems are down. We are assessing the situation. The safety of your business and our people is our top priority. We will update when we have more information.

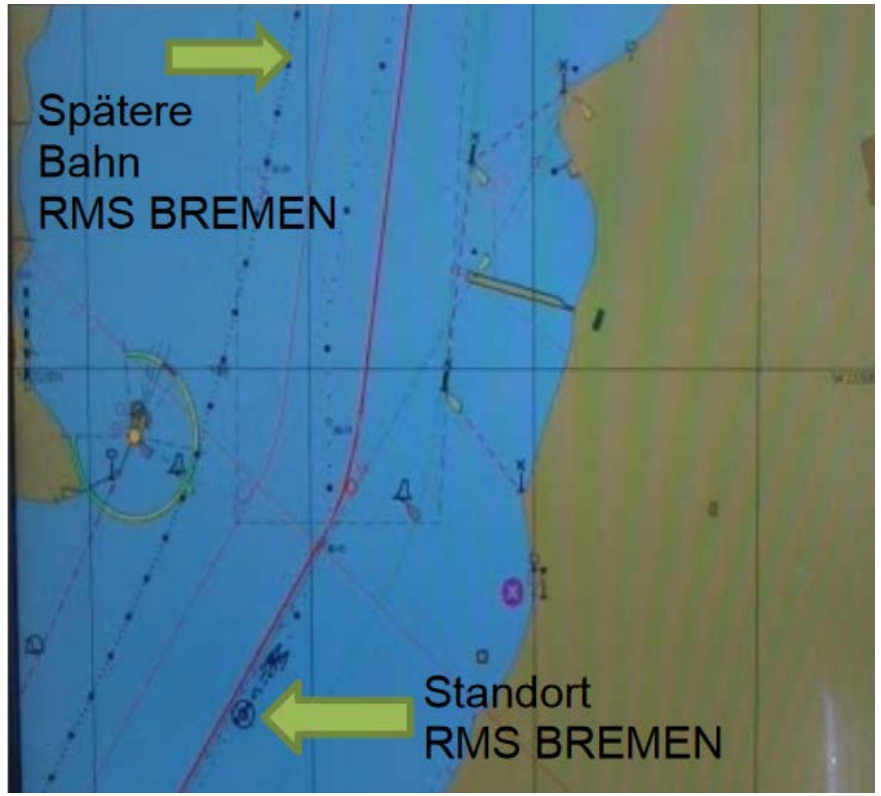
NotPetya: Kosten - 300m$
4k neue Server - 45k PC - 2,5k Applikationen

BSU
Bundesstelle für Seeunfalluntersuchung
Federal Bureau of Maritime Casualty Investigation

Az.: 276/14

1 Zusammenfassung

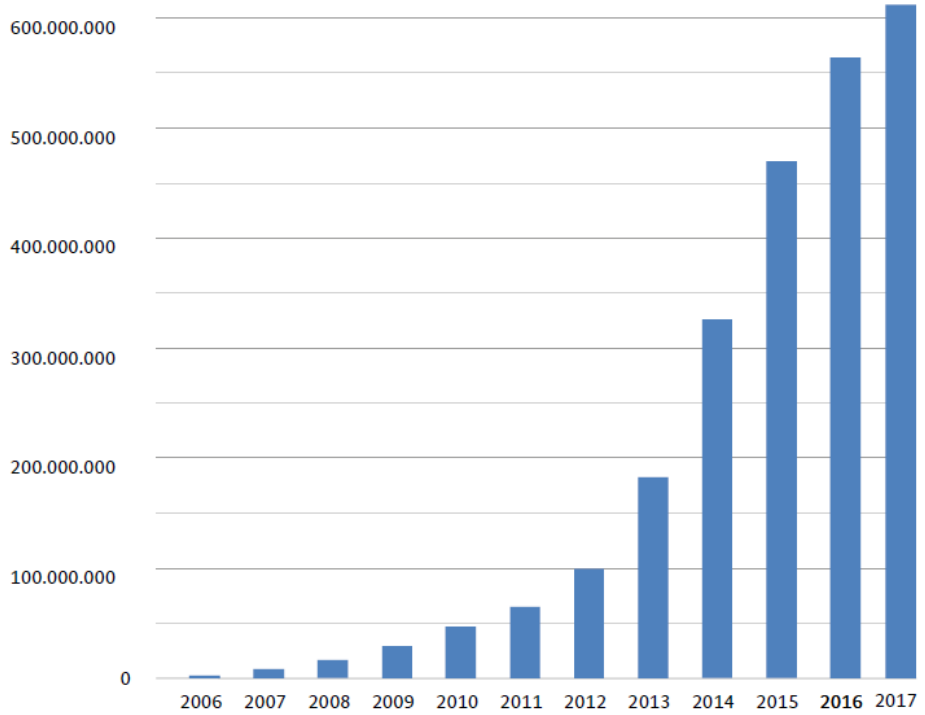
Am 5. September 2014 um 02:11 Uhr[1] kollidierte die unter zypriotischer Flagge ausgehende RMS BREMEN mit der unter Antigua & Barbuda Flagge einkommenden FRANCISCA auf der Höhe des Leuchtfeuers Friedrichsort in der Kieler Förde. Der genaue Kollisionsort bleibt unklar. Beide Fahrzeuge fuhren nach den AIS-Aufzeichnungen der Verkehrszentrale deutlich aneinander vorbei. Auf beiden Fahrzeugen befand sich eine elektronische Seekarte des Herstellers und Typs TRANSAS 4000 an Bord. Auch nach diesen Aufzeichnungen fuhren die Fahrzeuge aneinander vorbei.



Risiko?

- IT-Systeme an Bord genauso Cyber-Gefahren ausgesetzt wie Landsysteme.
- Ausbreitung von Cyber-Angriffen im Bordnetz genauso wie an Land.
- Schadprogramm durch mobile Geräte sehr leicht verbreitet.
- Cyber Kriminalität lukratives Geschäfts-modell für organisiertes Verbrechen.
- Cyber Sicherheit benötigt einen kontinuierlichen Prozess.
- Gezielte Cyber-Attacken auf Schiffe ???

$$Risiko = Eintrittswahrscheinlichkeit \cdot Schadensausmaß$$

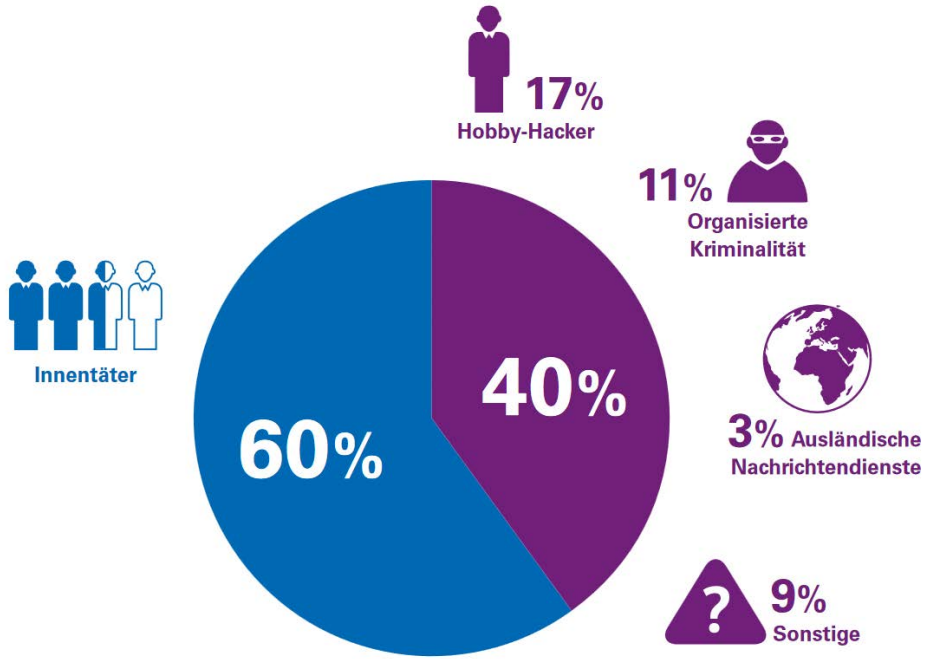


Bekannte Schadprogramme (2017 erwartet)

[Quelle: Helmut Weisskopf, BSI]

Aktuelle Situation

- Studie 2017 (IHS Fairplay – n=284):
  - 34% haben einen Cyber-Angriff erfahren
  - 30% ohne Manager/Abteilung für Informationssicherheit
  - 66% IT-Sicherheitsrichtlinie (Einführungsprozess?)
  - 47% größte Cyber-Schwachstelle sind Mitarbeiter (Awareness-Schulungen!)

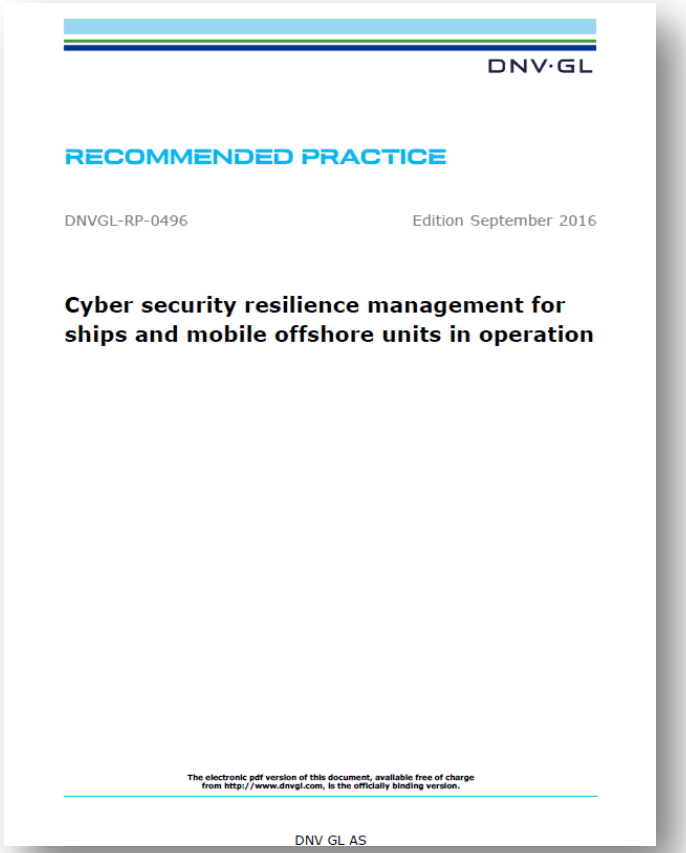


Der typische Cyber-Kriminelle ist
- mit 60-% Wahrscheinlichkeit Innentäter, also Teil der Organisation, die er angreift,
- männlich und zwischen Mitte 30 bis Mitte 50 Jahre alt,
- bereits mindestens 6 Jahre im Unternehmen beschäftigt,
- meist eine Führungskraft,
- eine respektierte, freundliche Person.

[Quelle: Digitalisierung und Cyber | Studie 2017, KPMG]

Was tun?

- Umfassende Betrachtung der Schiffsbetriebsprozesse


DNV·GL

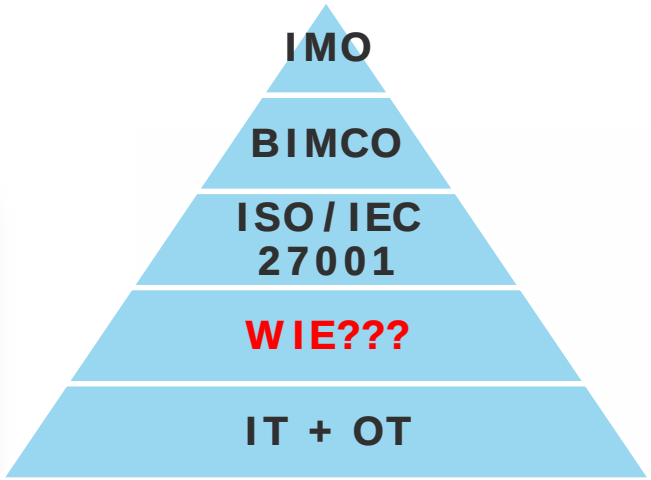
RECOMMENDED PRACTICE

DNVGL-RP-0496 Edition September 2016

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

The electronic pdf version of this document, available free of charge from http://www.dnvgl.com, is the officially binding version.

DNV GL AS



Processes

- Management systems
- Governance frameworks
- Policies and procedures
- Vendor/third-party contracts follow-up
- Audit regimes

People

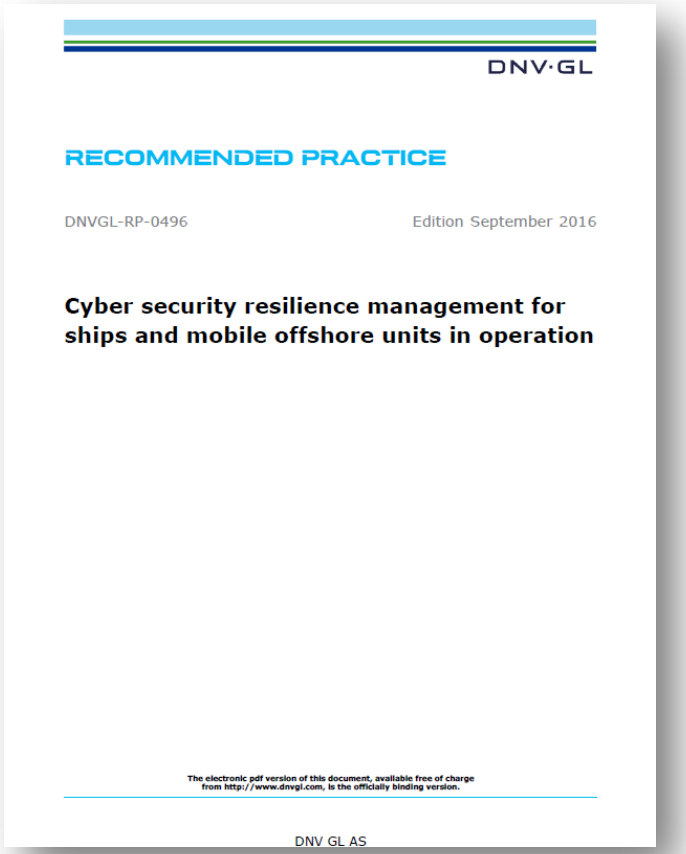
- Training and awareness
- Professional skills and qualifications
- Emergency drills
- Authorizations and authentication
- Physical security

Technology

- System design
- Hardening of connections
- Software configuration
- Encryption protocols
- Jamming and spoofing
- Detection and monitoring

Was tun?

- Umfassende Betrachtung der Schiffsbetriebsprozesse


DNV·GL

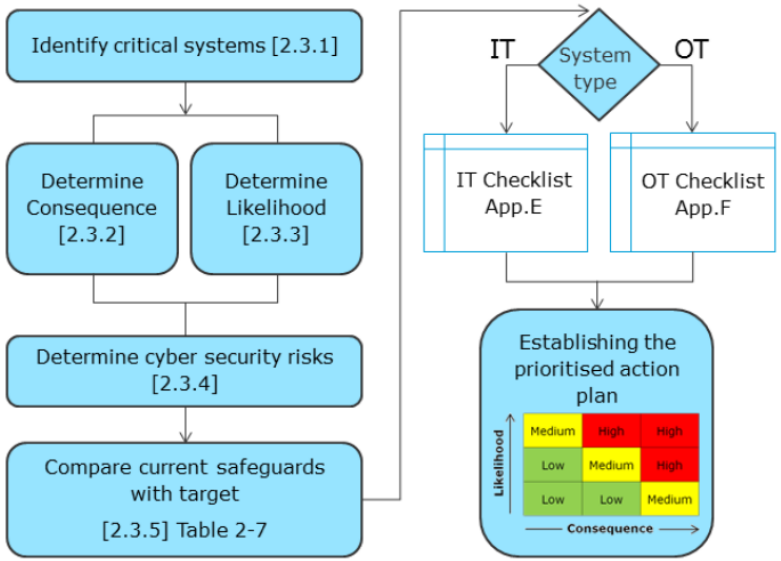
RECOMMENDED PRACTICE

DNVGL-RP-0496 Edition September 2016

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

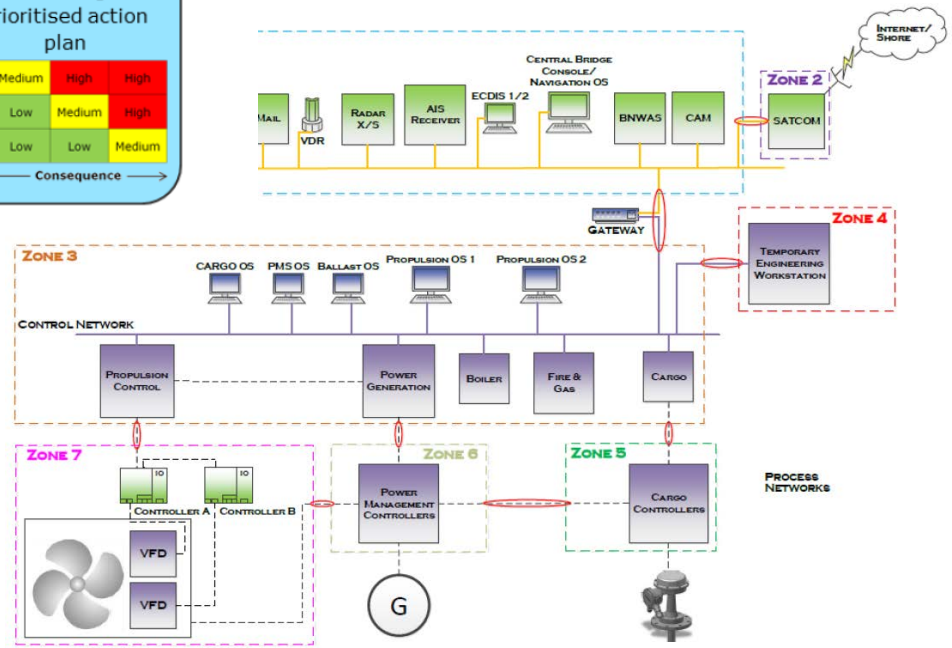
The electronic pdf version of this document, available free of charge from http://www.dnvgl.com, is the officially binding version.

DNV GL AS



Umfassende, detaillierte Bewertungsschritte.

Beispiel einer Netz-topologie für einen LNG-Tanker.



Im Schiffsbetrieb

Physikalische Aspekte		Digitalisierung
Risikobeurteilung	→	Cyber-Risikobewertung
Feuerübungen	→	Systemwiederherstellungsübung
Arbeitserlaubnis	→	Software Changemanagement
Zeichnungen	→	Software Topologie
Tests/ Prüfungen	→	Penetrationstests
Managementsysteme	→	ISMS
Ausbildung	→	Awareness-Schulungen

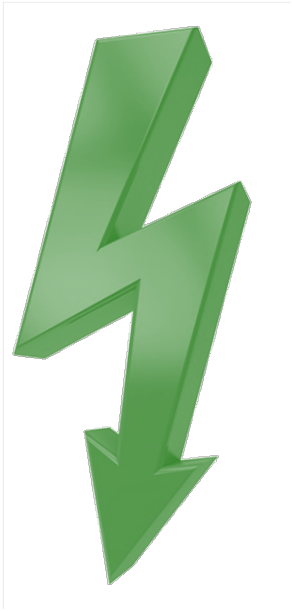
[Quelle: Svante Einarsson, DNV GL]

Fachpersonal an Bord:

- Schiffselektrotechnik Offiziere (HS Wismar, Bereich Seefahrt) mit Modulen **Technische Informatik, Programmierung, Gerätetechnik, Steuerungs- und Leittechnik, Kommunikationstechnik, Informationsübertragung …**

Spannungsfeld

Digitalisierung & Mobile Anwendung	Einfallstor für Angriffe
Innovation(en)	Sicherheit
Schiffe „always on“	Software Update-Management an Bord
Daten in der Clowd verfügbar	Daten lukratives Ziel
Effizientes Arbeiten an Bord	Einhalten von Sicherheitsvorgaben
Schiffsbetriebstechniker	Schiffselektrotechniker



Vielen Dank für Ihre Aufmerksamkeit.

www.dnvgl.com

SAFER, SMARTER, GREENER