Maritime Cyber Security

Cyber Security and Shipping

October 19th 2017

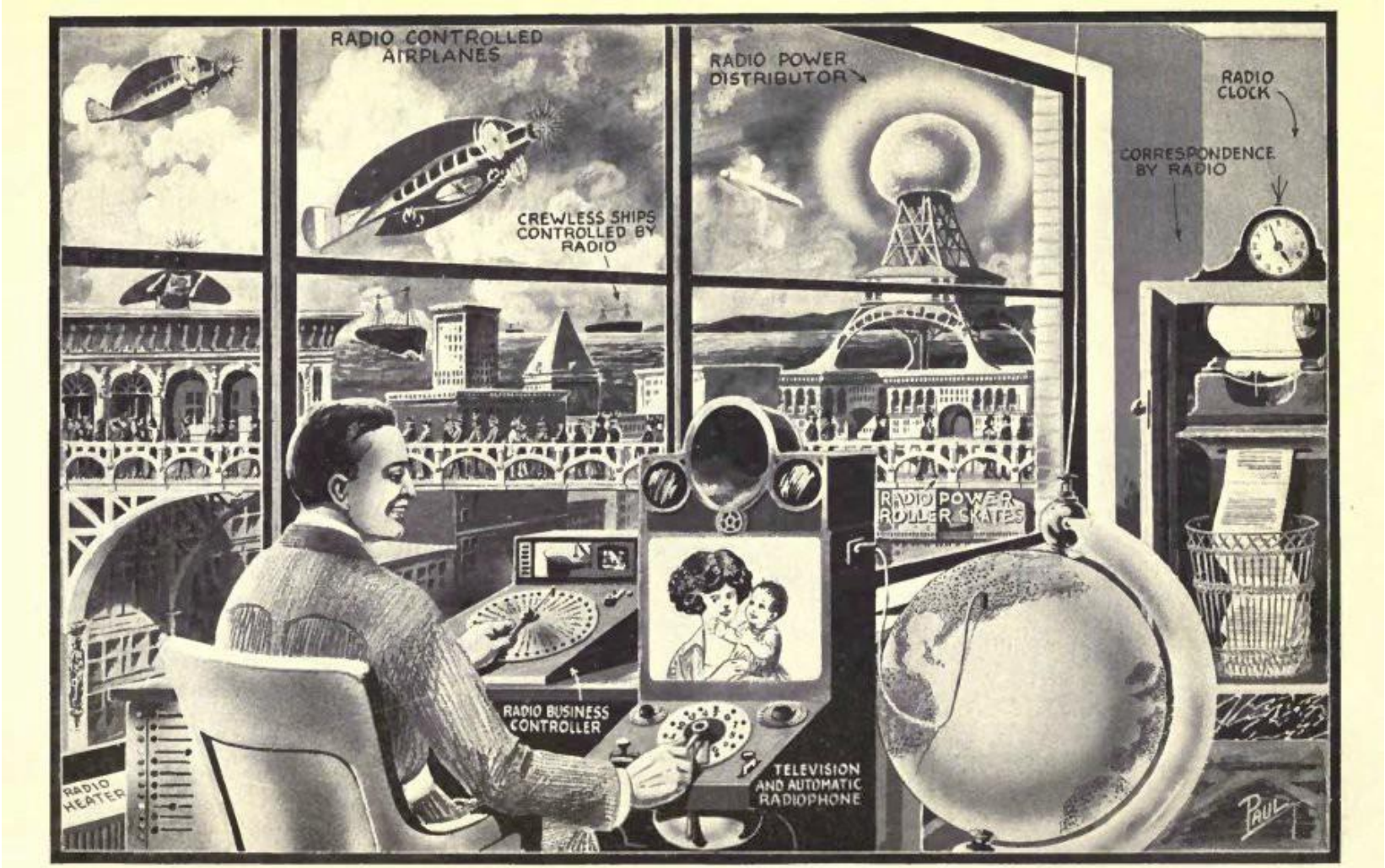
DNV GL MARITIME ADVISORY

PATRICK ROSSI – CYBER SECURITY SERVICE MANAGER

Pirates 1.0 → 4.0

Photo: Shutterstock

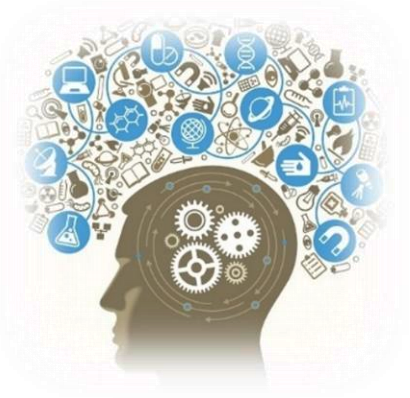
Being the early adopter…



Hugo Gernsback (1884-1967) Luxembourgish-American inventor, writer, editor, publisher, best known for publications including the first science fiction magazine.

Risk misconception and industry lack of understanding

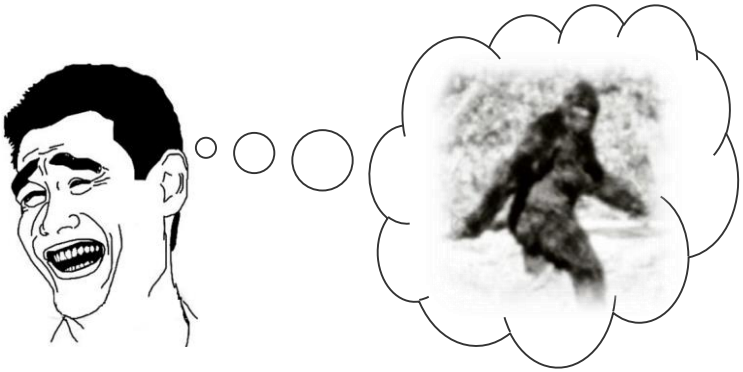
- Difficulty in calculating risks linked to the thinking of the human criminal mind



RISK
=
IMPACT
X
LIKELYHOOD <-?

- Disbelief

  "… a hacker gained control of a vessel…"



"Yeah Right, there are too many barriers to get through…"

WannaCry: Largest ransomware attack to date

Known affected organisations:

- Spain - Telefonica, power firm Iberdrola, utility provider Gas Natura and more large firms
- USA - FedEx,
- France - Renault,
- Germany - Deutsche Bahn
- Jakarta- Two hospitals
- Russian Interior Ministry
- Britain's National Health Service, Nissan car plant

"The latest count is over 200,000 victims in at least 150 countries"

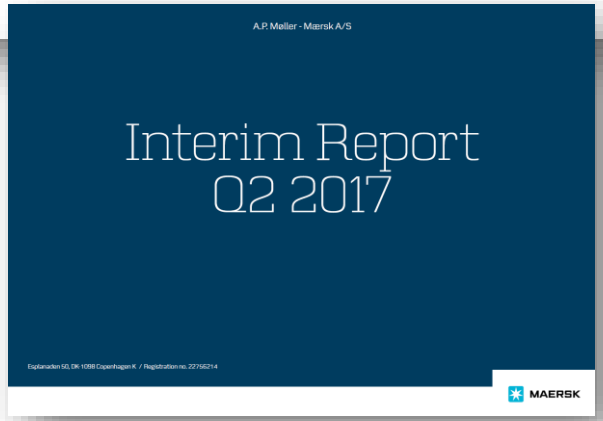
- Rob Wainwright, Europol Executive Director

Maritime can also affected

Corporate Earnings Show Impacts of NotPetya Cyber Attack

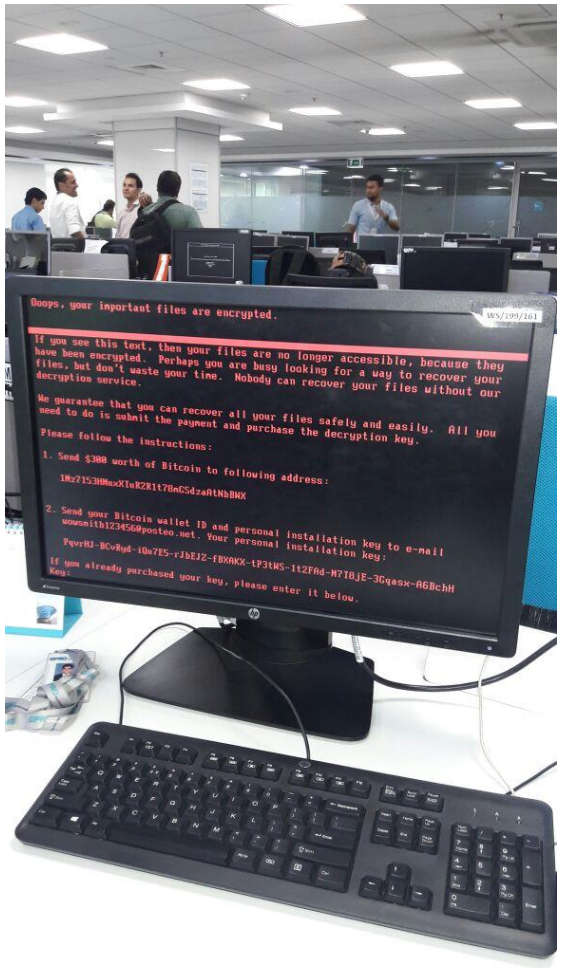
August 2, 2017 by Reuters

Transport & Logistics reiterates the expectation of an underlying profit above USD 1bn, despite expected negative result impact from the June cyber-attack estimated at a level of USD 200-300m, of which the majority relates to lost revenue in July. The vast majority of the impact of the cyber-attack was in Maersk Line.



NotPETYA: Heavily impacting maritime industry players

- Arrived via an update to an accounting system in Ukraine (ME Doc)
- Spread like a worm from an infected machine
- Exploited Windows SMB vulnerability (aka EternalBlue), fix by Microsoft was released on March 14th (MS17-010)
- Spreads into the local network using exploits like Eternal Blue and tools like PsExec and WMIC
- Encrypts MFT (Master File Tree) tables for NTFS partitions
- Overwrites the MBR (Master Boot Record) with a custom bootloader
- Shows a ransom note demanding USD 300, same bitcoin wallet
- Prevents victims from booting their computer



"Big hack at Maersk puts Rotterdam's container terminal flat"
David Bremmer and Leon van Heel, AD, NL

NotPETYA: Heavily impacting maritime industry players

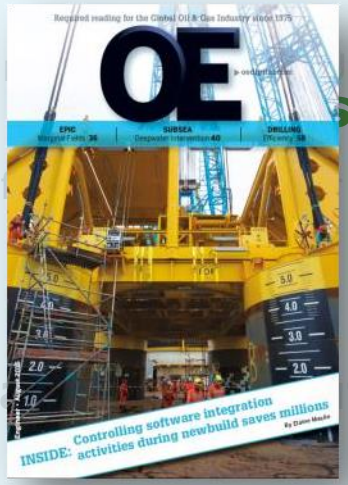
- Arrived via an update to an accounting system in Ukraine (ME Doc)
- Spread like a worm from an infected machine
- Exploited Windows SMB vulnerability (aka EternalBlue), fix by Microsoft was released on March 14 (MS17-010)
- Spreads into the local network using exploits like Eternal Blue and tools like PsExec and WMIC
- Encrypts MFT (Master File Table) tables for NTFS partitions
- Overwrites the MBR (Master Boot Record) with a custom bootloader
- Shows a ransom [illegible] wallet
- Prevents victims [illegible]

Software Configuration management ?

Software Patch management ?

Obsolescence management ?

Integrated Software Dependent Systems (ISDS)



"Big hack [illegible] terminal flat"

[illegible] Heel, AD, NL

On board Cyber Security inspections

Surveyors find viruses on-board during routine inspections…

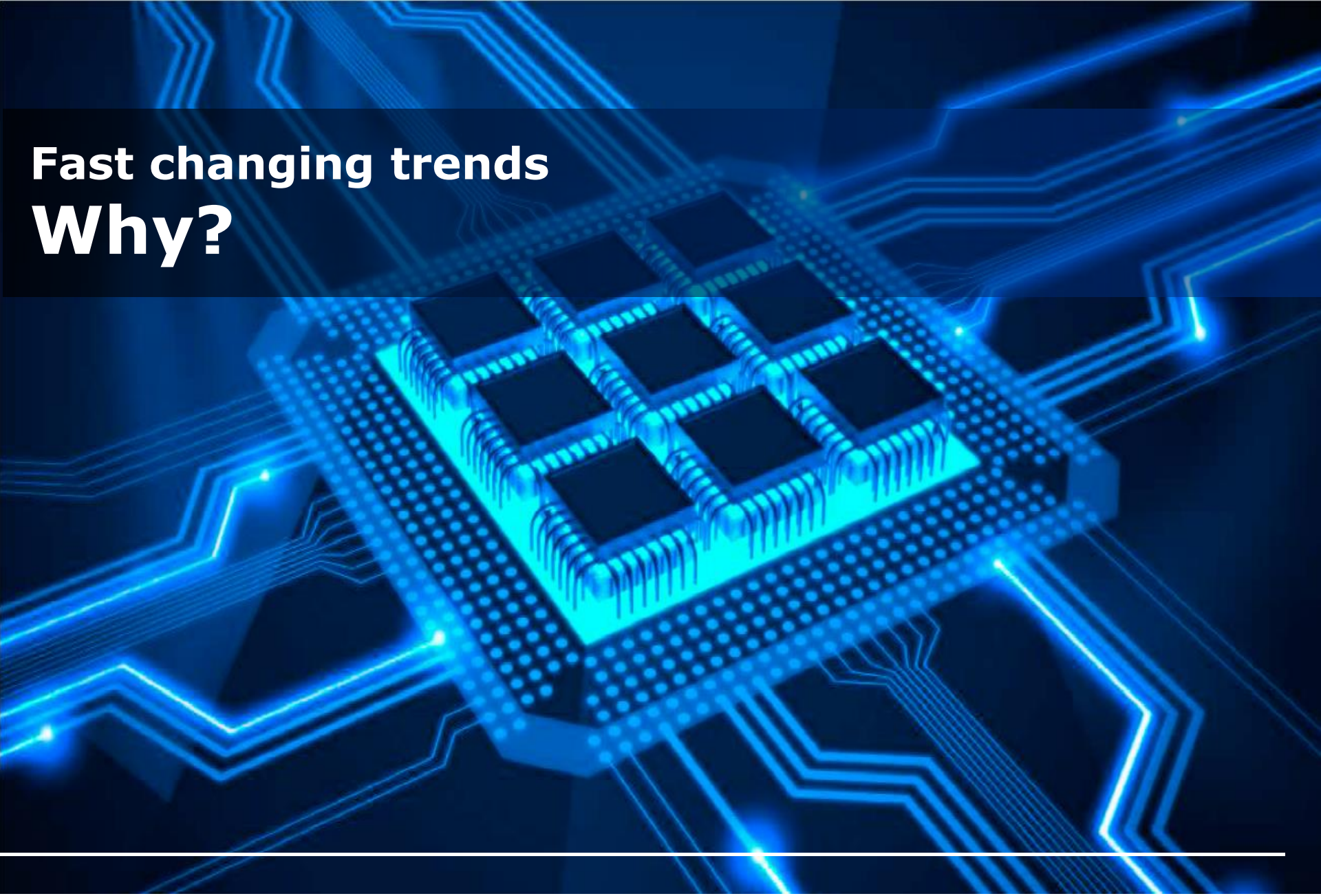
Transparency VS Awareness…

"There are two types of companies in the world: those that know they've been hacked, and those that don't".

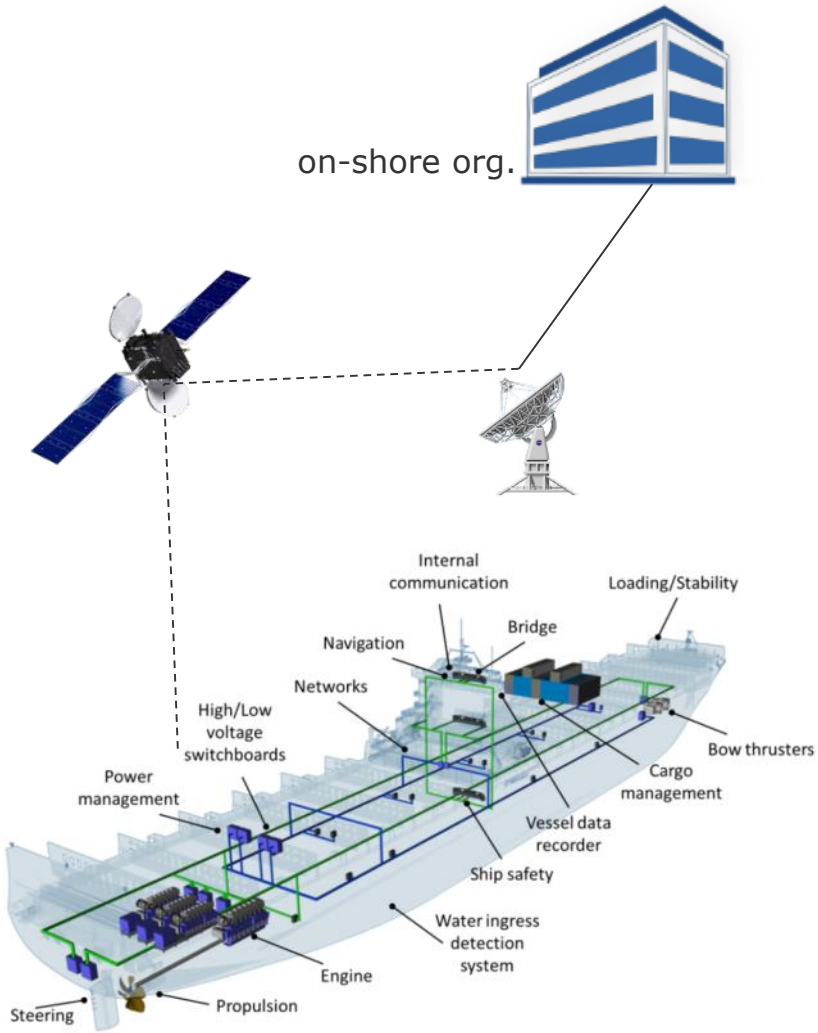
Misha Glenny, British journalist who specialises in cybersecurity

Cyber security incidents are more common than officially admitted..

Fast changing trends
Why?



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…

At risk:

Mainly finance and reputation

Operation Technology (OT)

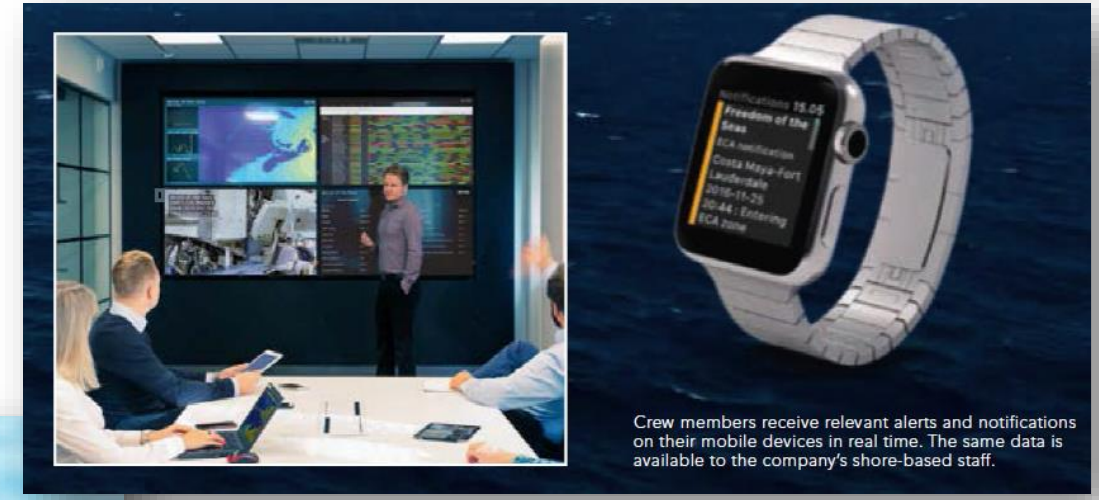
- PLCs
- SCADA
- On-board measurement and control
- ECDIS
- GPS
- Remote support for engines
- Data loggers
- Engine & Cargo control
- Dynamic positioning, …

At risk:

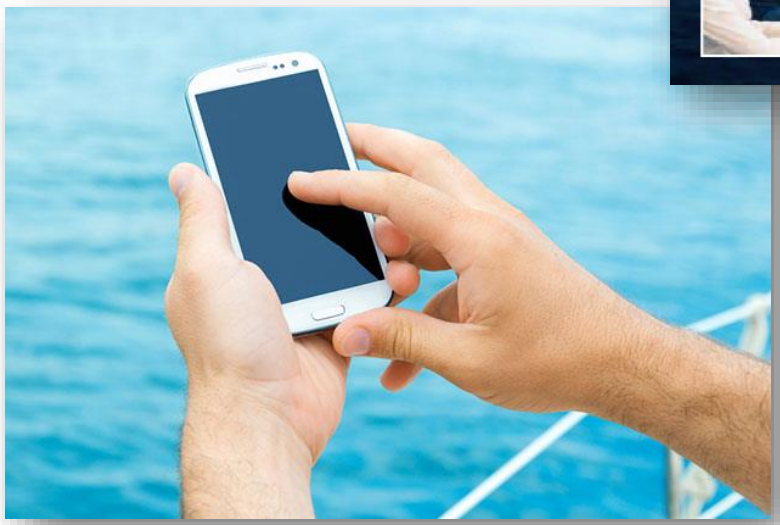
Life, property and environment + all of the above

The future holds more…

Digital wearables for crew



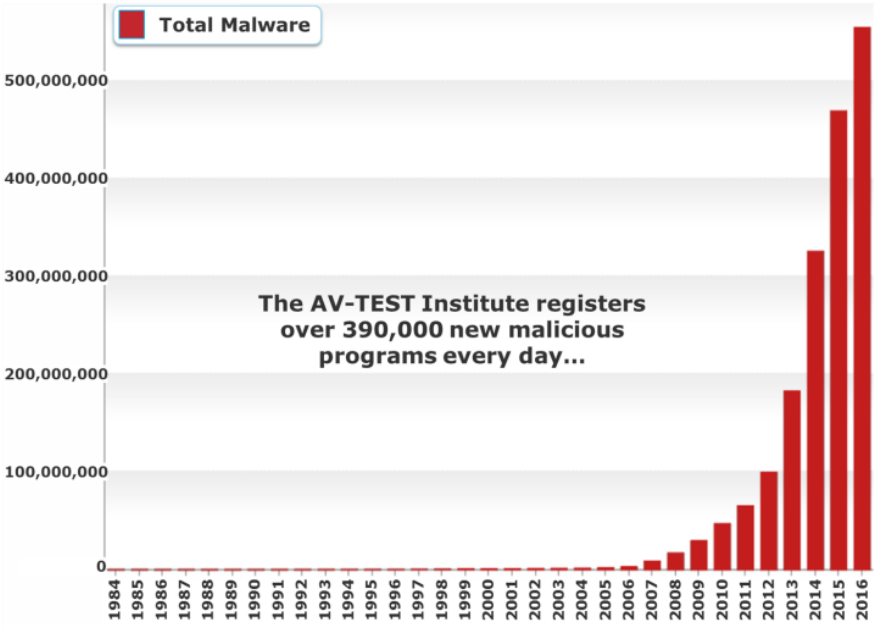
Crew members receive relevant alerts and notifications on their mobile devices in real time. The same data is available to the company's shore-based staff.



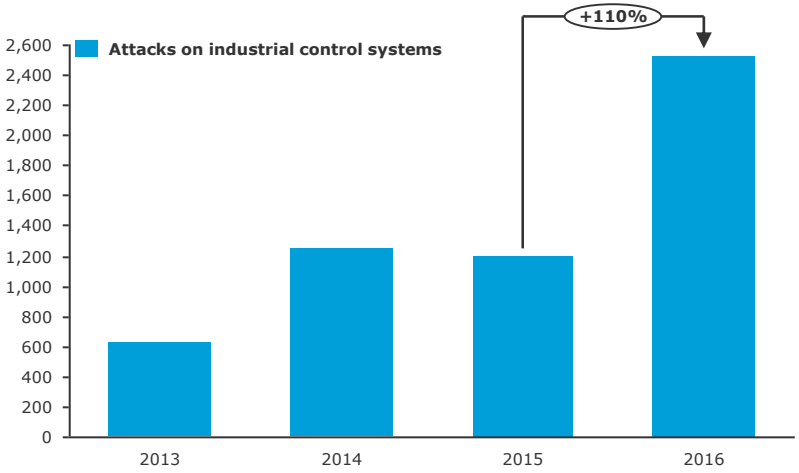
Increasing number of interfacing devices

Cyber security may not be at the top of every fleet managers agenda, but it is probable to climb as issues migrate to OT world

Information technology (IT)



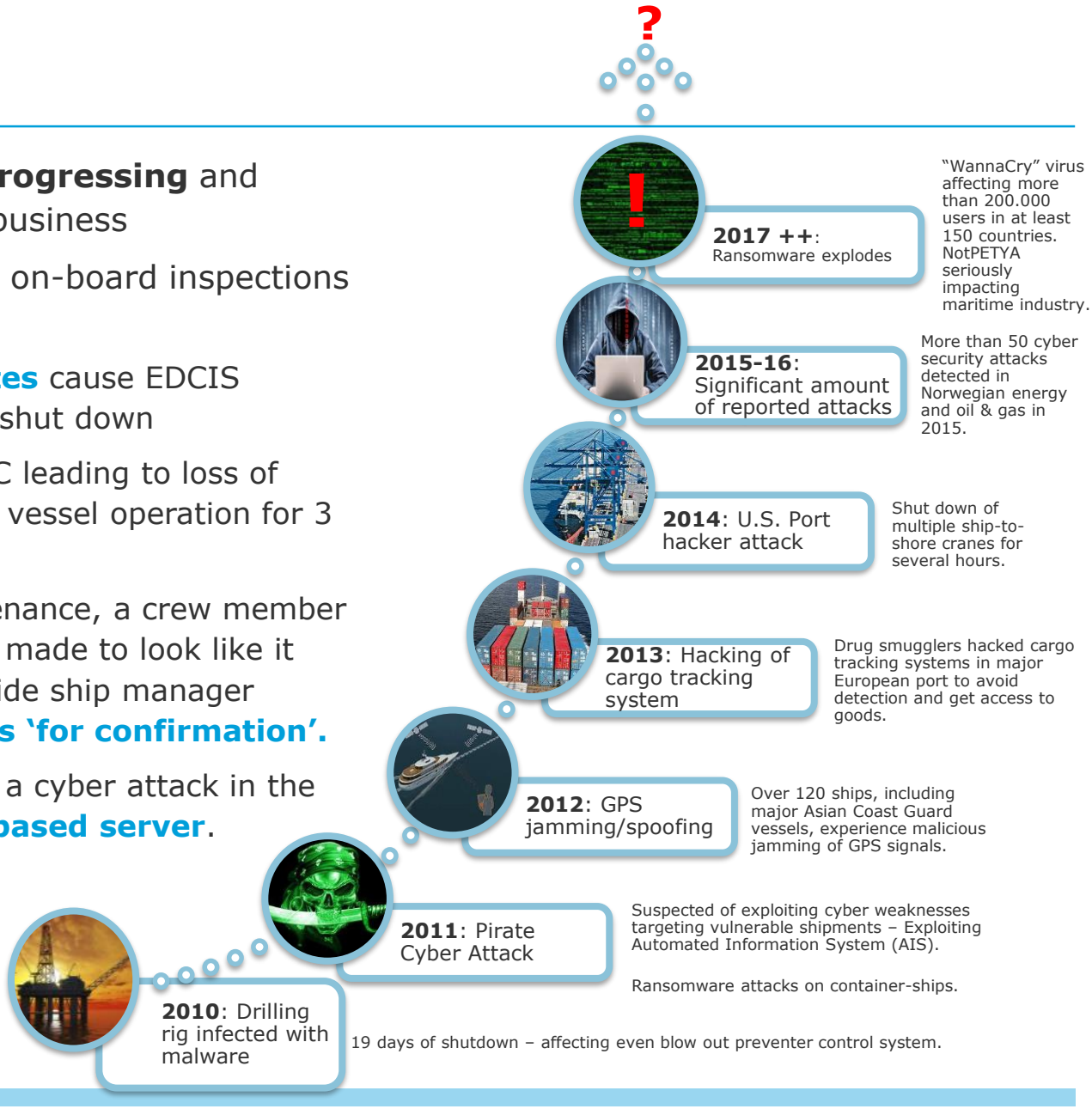
Operational technology (OT)



Source: AV-TEST Institute, Germany & IBM Managed Security Services
OT: Operational Technology such as Industrial Control Systems, SCADA, PLCs, Sensors
SCADA : Supervisory Control and Data Acquisition (Operator control and monitoring systems)

Trends

- Cyber security **threats are progressing** and becoming a part of our daily business
- Some examples from DNV GL on-board inspections and work with clients:
  - Infected **ECDIS chart updates** cause EDCIS systems of 2 bulk carriers to shut down
  - **Ransomware** on master's PC leading to loss of main switchboard and loss of vessel operation for 3 days.
  - While ongoing routine maintenance, a crew member of a vessel received an email made to look like it was coming from the shore side ship manager asking for system **passwords 'for confirmation'.**
  - A shipping company suffered a cyber attack in the office directed at the **shore-based server**. With corrupted data also on **vessel** as consequence.



National developments

- Development of maritime regulations since Sept 2016
- Require incident reporting since Jan 2017
- Draft navigation and vessel inspection circular NVIC 05-17 (hearing)

- Recommondations on maritime cyber security from Sept 2016

- Norwegian Maritime Authorities' report "Digital vulnerabilities in the maritime sector" by DNV GL from April 2015

- Dutch Data Processing and Cybersecurity Notification Obligation Act, since Jan 2017

- Development of Japanese guideline for cyber security applicable to maritime assets supported by DNV GL since 2016

- IT-Sicherheitsgesetz from June 2015 – includes ports but not ships

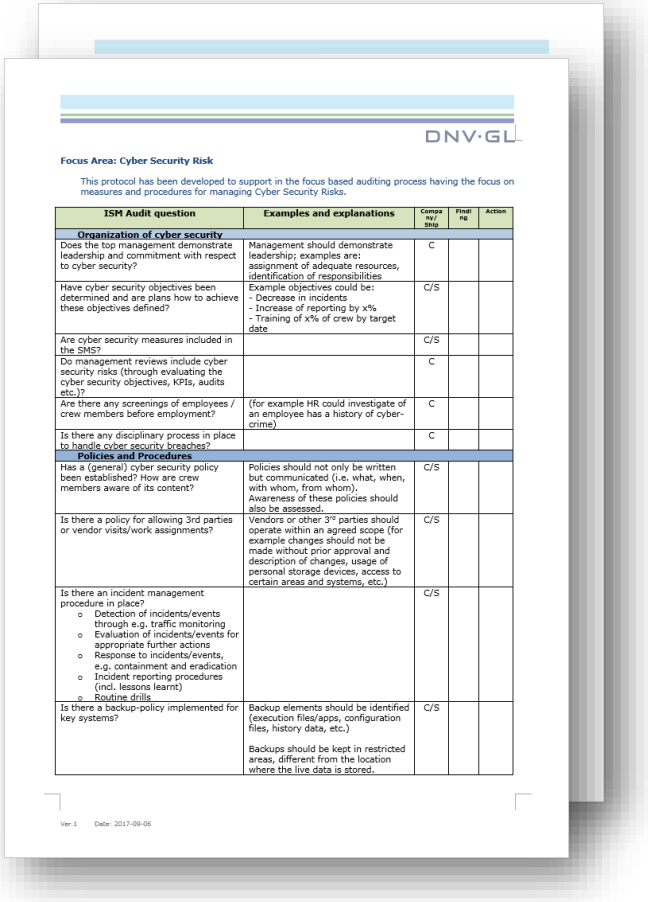
IMO and EU regulations

- Directive (EU)2016/1148 concerning measures for a high common level of security of network and information systems across the Union from May 2016
  – includes ports but not vessels
- Regulation (EU) 2016/679 - **General Data Protection Regulation (GDPR)** apply from May 2018
  - includes ships

- MSC/FAL.1/Circ.3 - Guidelines On Maritime Cyber Risk Management
  – Mandatory character
- MSC 98 adopted resolution MSC.428(98) on *Maritime cyber risk management in safety management systems*
  – MSC.428(98) encourages Administrations to ensure that cyber risks are appropriately addressed in safety management systems**, no later than the first annual verification of the company's Document of Compliance after 1 January 2021**.

DNV GL Cyber Security ISM audit checklist drafting

- Fit For Purpose Audit checklist



DNV·GL

Focus Area: Cyber Security Risk

This protocol has been developed to support in the focus based auditing process having the focus on measures and procedures for managing Cyber Security Risks.

ISM Audit question	Examples and explanations	Company/ Ship	Finding	Action
Organization of cyber security				
Does the top management demonstrate leadership and commitment with respect to cyber security?	Management should demonstrate leadership; examples are: assignment of adequate resources, identification of responsibilities	C		
Have cyber security objectives been determined and are plans how to achieve these objectives defined?	Example objectives could be: - Decrease in incidents - Increase of reporting by x% - Training of x% of crew by target date	C/S		
Are cyber security measures included in the SMS?		C/S		
Do management reviews include cyber security risks (through evaluating the cyber security objectives, KPIs, audits etc.)?		C		
Are there any screenings of employees / crew members before employment?	(for example HR could investigate of an employee has a history of cyber-crime)	C		
Is there any disciplinary process in place to handle cyber security breaches?		C		
Policies and Procedures				
Has a (general) cyber security policy been established? How are crew members aware of its content?	Policies should not only be written but communicated (i.e. what, when, with whom, from whom). Awareness of these policies should also be assessed.	C/S		
Is there a policy for allowing 3rd parties or vendor visits/work assignments?	Vendors or other 3rd parties should operate within an agreed scope (for example changes should not be made without prior approval and description of changes, usage of personal storage devices, access to certain areas and systems, etc.)	C/S		
Is there an incident management procedure in place? o Detection of incidents/events through e.g. traffic monitoring o Evaluation of incidents/events for appropriate further actions o Response to incidents/events, e.g. containment and eradication o Incident reporting procedures (incl. lessons learnt) o Routine drills		C/S		
Is there a backup-policy implemented for key systems?	Backup elements should be identified (execution files/apps, configuration files, history data, etc.) Backups should be kept in restricted areas, different from the location where the live data is stored.	C/S		

Ver: 1 Date: 2017-09-06

Check list categories (draft):

- Organization of cyber security
- Policies and Procedures
- Cyber security risk management
- Training and awareness
- Physical security and access control
- Network security

ISM Audit question	Examples and explanations	Company/ Ship	Finding	Action

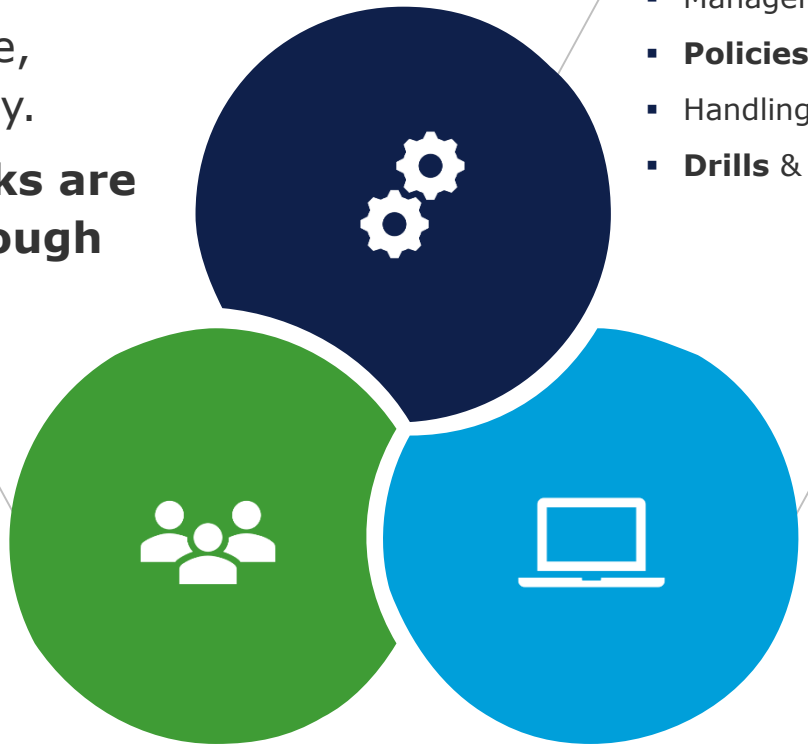
Countering Cyber risks is not that mysterious

The ship management industry already addresses risks throughout the dimensions of People, Process & Technology.

Cyber Security risks are also managed through these:

Process

- Management Systems
- **Policies, Procedures**
- Handling of Vendor/Third parties
- **Drills** & Audit regimes



People

- **Cyber Hygiene**
- Training & Awareness
- Professional skills & qualifications
- **Written procedures**
- Authorization control
- **Physical Security**

Technology

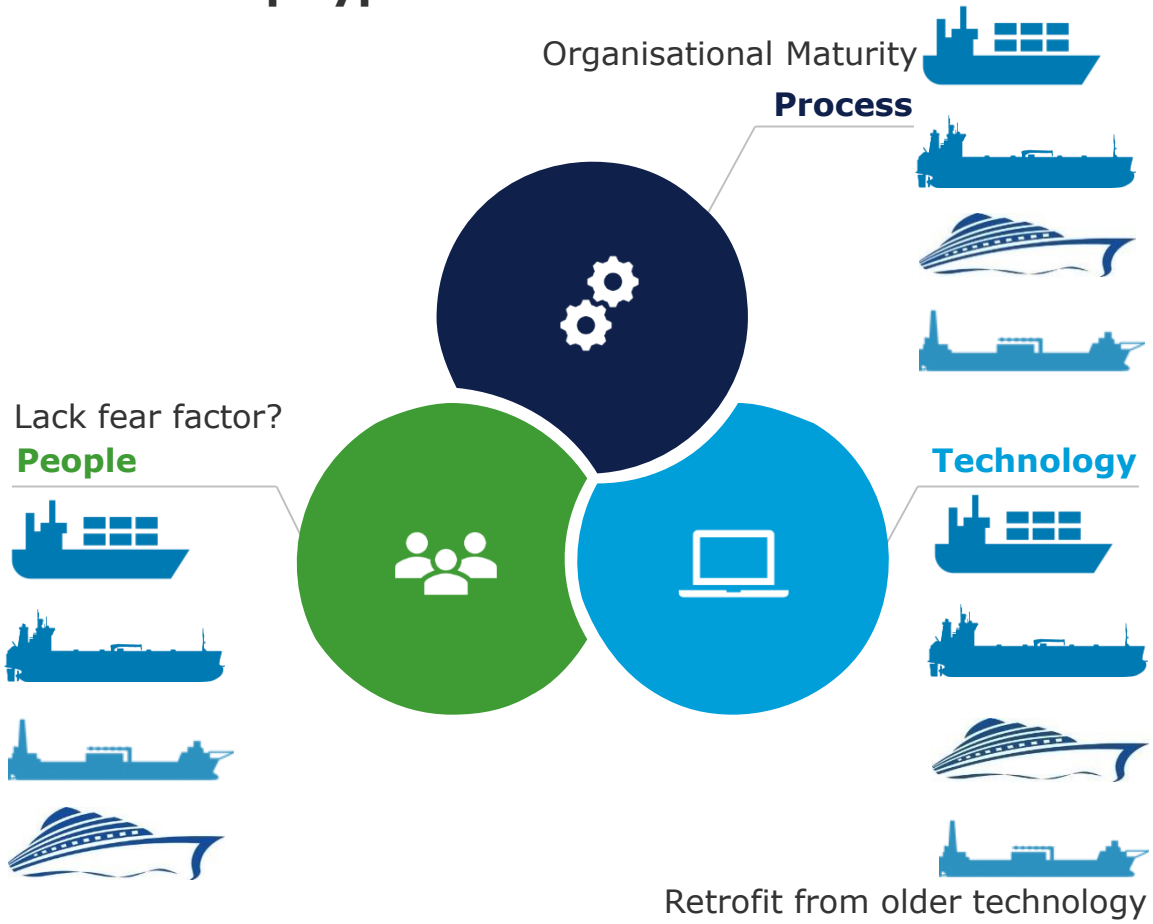
- Antivirus
- Firewalls
- Intrusion detection systems
- **SW update, Patches**
- Test
  - Functional testing
  - Vulnerability Scanning
  - **Penetration test**

Cyber Sec on-board inspections
What findings?

On board verification tests and inspections

Categories of findings on different ship types:

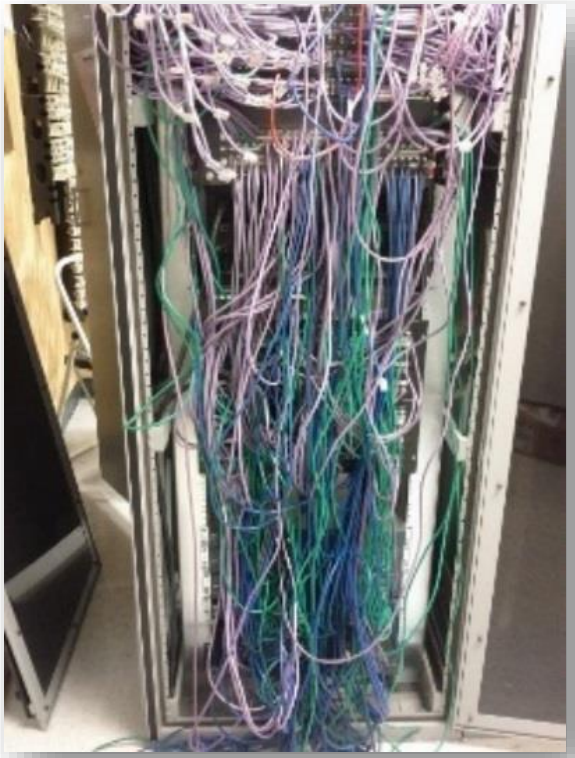
- **People, Process, Technology**
  - Passenger, Container, Tanker, Offshore production unit



Example findings on Passenger, Container, Tanker & Offshore production units

- Network Security

Are firewalls used according to policy?



- Firewall mounted in engine performance monitoring cabinet, but not connected

Example findings (cont.)

- Network Security

Are anti-virus used according to policy?

- No Anti-virus on "island-mode" workstations

- Skype installed on tank sounding computer
- Undetected infection of Loading computer

Example findings (cont.)

- Physical security and access control

Checking access control

- No password change policy, passwords pre-set by shore IT
  - Passwords printed on paper and posted on the wall
- **Unnecessary Administrator access** on engine performance monitoring PC
- **No automatic lock out**, and users stay logged in to workstations, because reporting tasks are so time consuming that they cannot be handled by a single person
- **Lack of physical security**, all equipment in scope is accessible
- Weak passwords, e.g. “123”

Example findings (cont.)

- Network Security

Network Security checks

- Personal use of company network
  - E-mail (**bypassing corporate filtering**), browsing, and **social networking** on on-board PCs
- 4 **base functions of on-board firewall disabled**, including event-logging & Broadcast storm protection disabled in switches
- Limited alarm and event logging
  - Security products generate alarms, **but there is no central collection or review of events**
- **Lack** of Windows patching & **hardening**
  - Windows updated only during major upgrades, i.e. **up to 3 years outdated.**
  - Windows installations configured with **standard settings**
  - **Default credentials on networking gear,** e.g. switches, routers
- **15 Anti-virus alarms in a week on sample PC on-board**

Example findings (cont.)

- Network Security

Network Security checks

- Anti-virus installed on all hosts: However, **no scheduled scans**. Last scan in 2014
- **No monitoring/alarming of network load** within Network panel of Alarm server HMI
- Alarm servers running **unused/unnecessary services**
- Adequate malware **protection not installed on HMI PCs** (Alarm monitoring and Engine Performance monitoring)
- Alarm **overflow**: After a certain number, **no further alarms can be received**
- OS security patches ~twice a year (except ship's firewall)
- **Unencrypted e-mail communication**

Example findings (cont.)

- Policies and Procedures

Checks on policies and procedures

- No **defined policies** to follow by associated **vendors**/service personnel
  - Service provider technician uses own USB stick to print reports from on-board PCs
- Dedicated USB stick for updating ECDIS, however physically not secured and no malware scanning
- Single USB stick policy
  - Single USB used to transfer loading condition data to shore via Bridge
  - SD card used between camera and on-board workstations
  - Gradually all of business network on-board infected

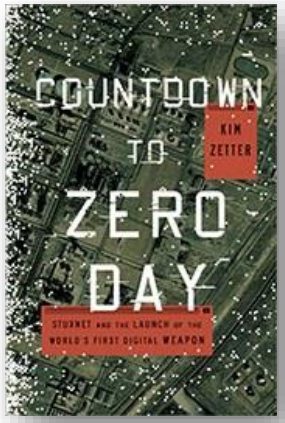
Example findings (cont.)

- Policies and Procedures

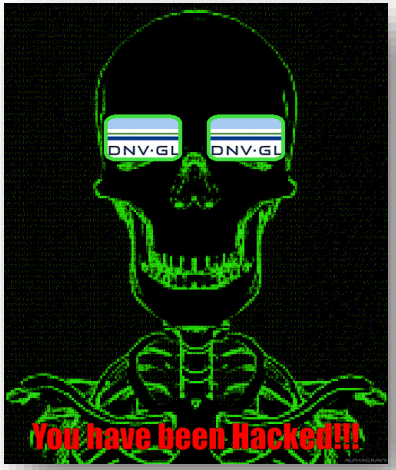
Checks on policies and procedures

- All data and configuration **backups stored in a single cabinet on-board**
- All backup HDDs **stored in a single rack** (together with all IT servers), and **not transferred to shore**
- IT dept. responsible for comm. networks, but Master is responsible on the vessel
  - **No incident response policy defined**. The Master would contact IT dept.
  - AIS kept on in piracy area despite policy to switch off: **No policy regarding sharing geo-tagged photos**

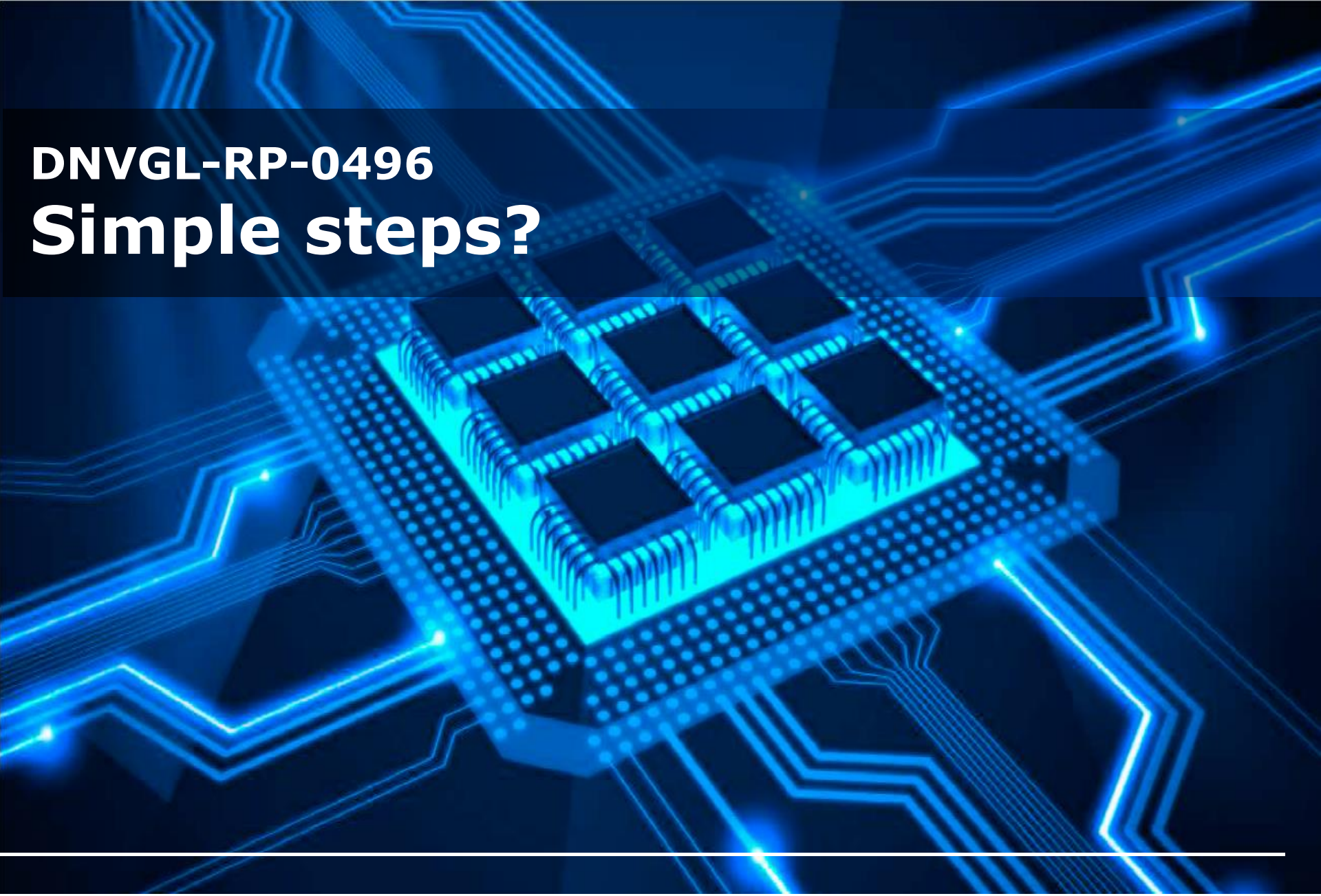
Clues from selfies can lead to self inflected issues…



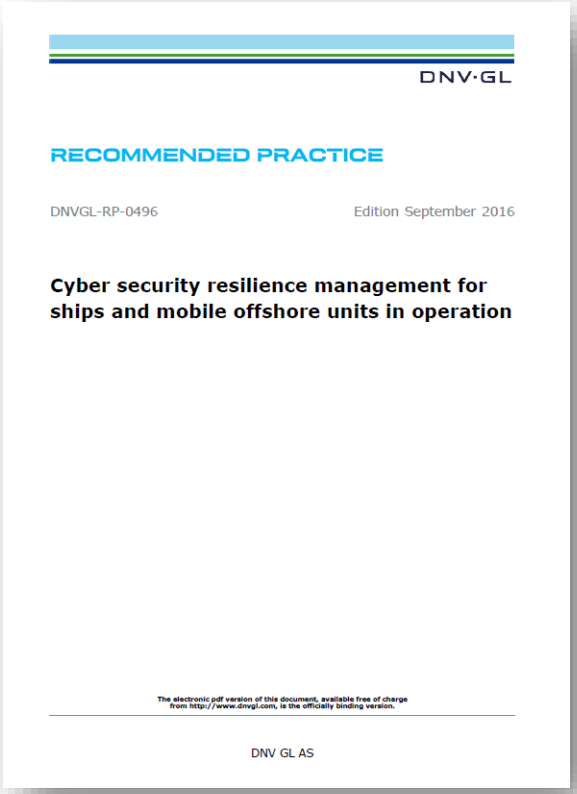
On board penetration test demo



DNVGL-RP-0496
Simple steps?



Industry response: Cyber Security guidance



DNV·GL

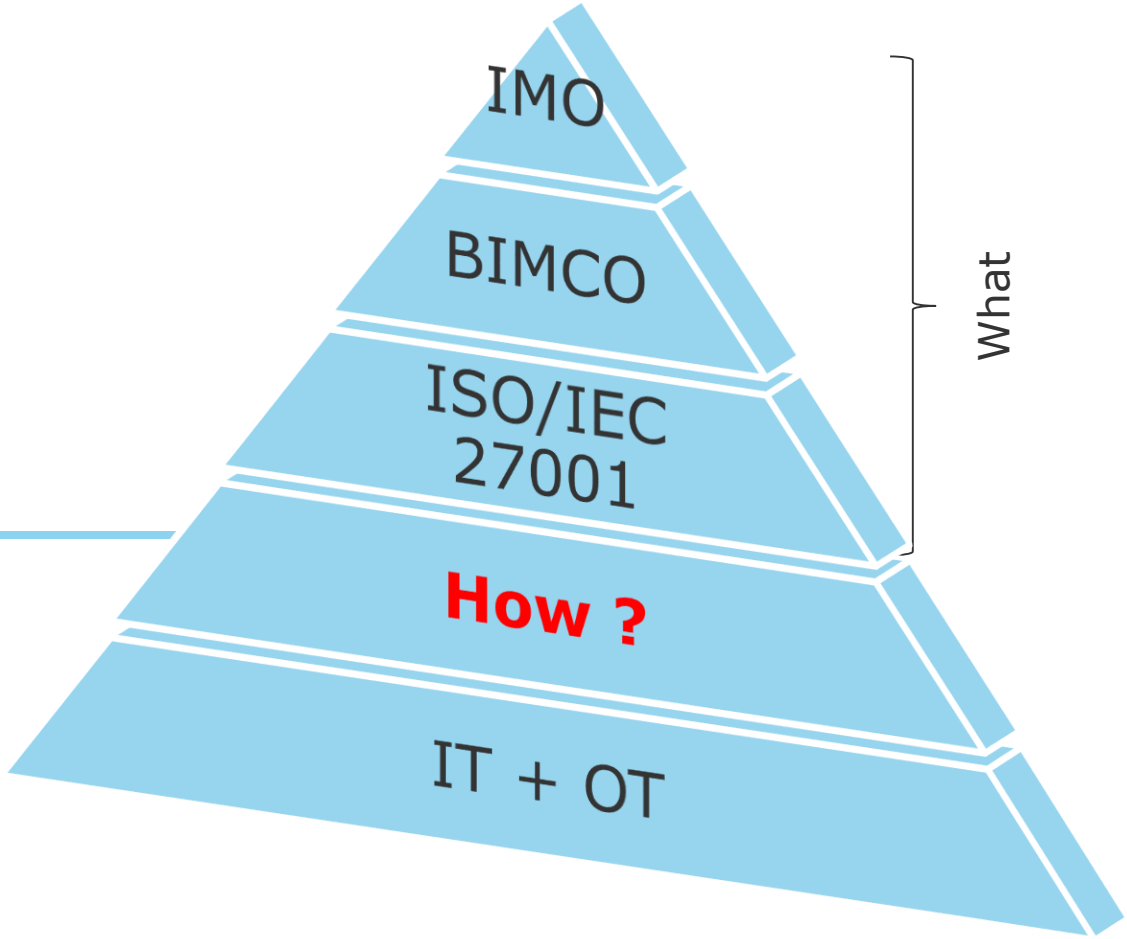
RECOMMENDED PRACTICE

DNVGL-RP-0496 Edition September 2016

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

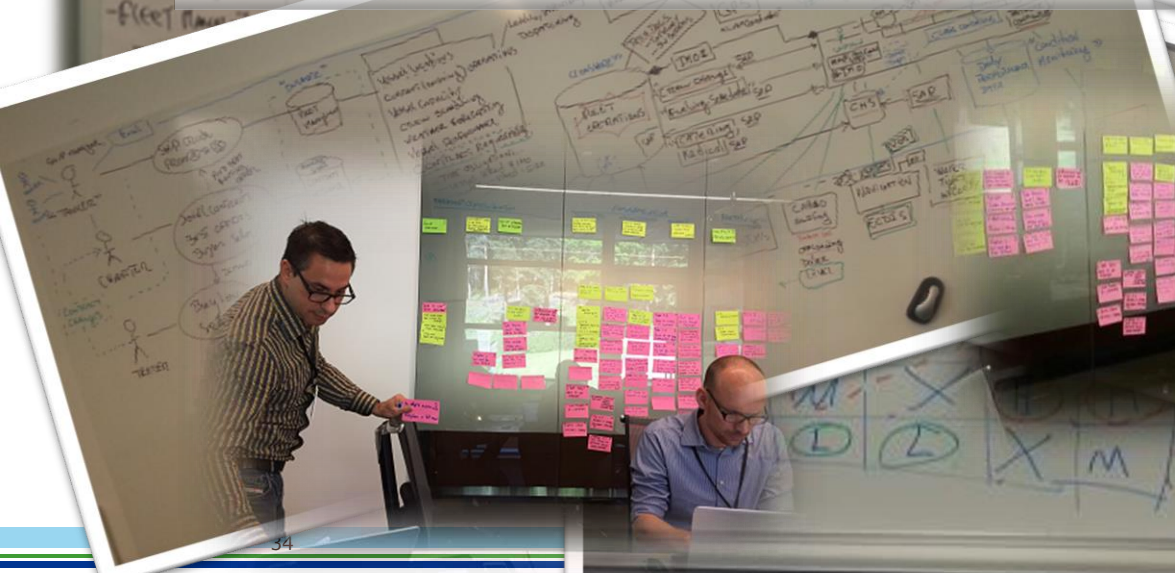
The electronic pdf version of this document, available free of charge from http://www.dnvgl.com, is the officially binding version.

DNV GL AS



RP: 14 Iterations with customers from all segments)

- Cross industry and cross discipline workgroup
- A number of representative external stakeholders used as reference group
- Learning from live cyber security projects
- 1000 comments received and addressed from internal and external cyber security experts
- First impression feedback from customers confirm that the RP is relevant, practical and needed



CYBER SECURITY DNVGL-RP-0496

"Looks really good, best CS guideline out there"
Passenger company

"We embrace this approach, thumbs up for the initiative"
Shipping manager

"This RP is absolutely useful in bridging the gap between the IT & OT* worlds"
Shipping manager

"Outstanding guidance that can be easily understood and embraced by most organizations"
Flag state

DNV·GL

RECOMMENDED PRACTICE
DNVGL-RP-0496

CYBER SECURITY RESILIENCE MANAGEMENT
FOR SHIPS AND MOBILE OFFSHORE UNITS IN OPERATION

DNV GL MARITIME

Doc Number: DNVGL-RP-0496

DNV GL Headquarters, Veritasveien 1, P.O.Box 300, 1322 Høvik, Norway. Tel: +47 67 57 99 00. www.dnvgl.com

DNV GL – www.dnvgl.com

This RP is a comprehensive document that provides a good approach to Cyber Security for ICS*"
Shipping manager

"This RP makes a lot of sense"
Shipping manager

"Generally very good approach and description of the requirements"
Gov. agency

"Good overview of the recommended process with supporting tables, examples, checklists etc. Overall well done!"
Shipping manager

*OT: Operational Technology (Automation, Sensors, Industrial Control Systems (ICS)

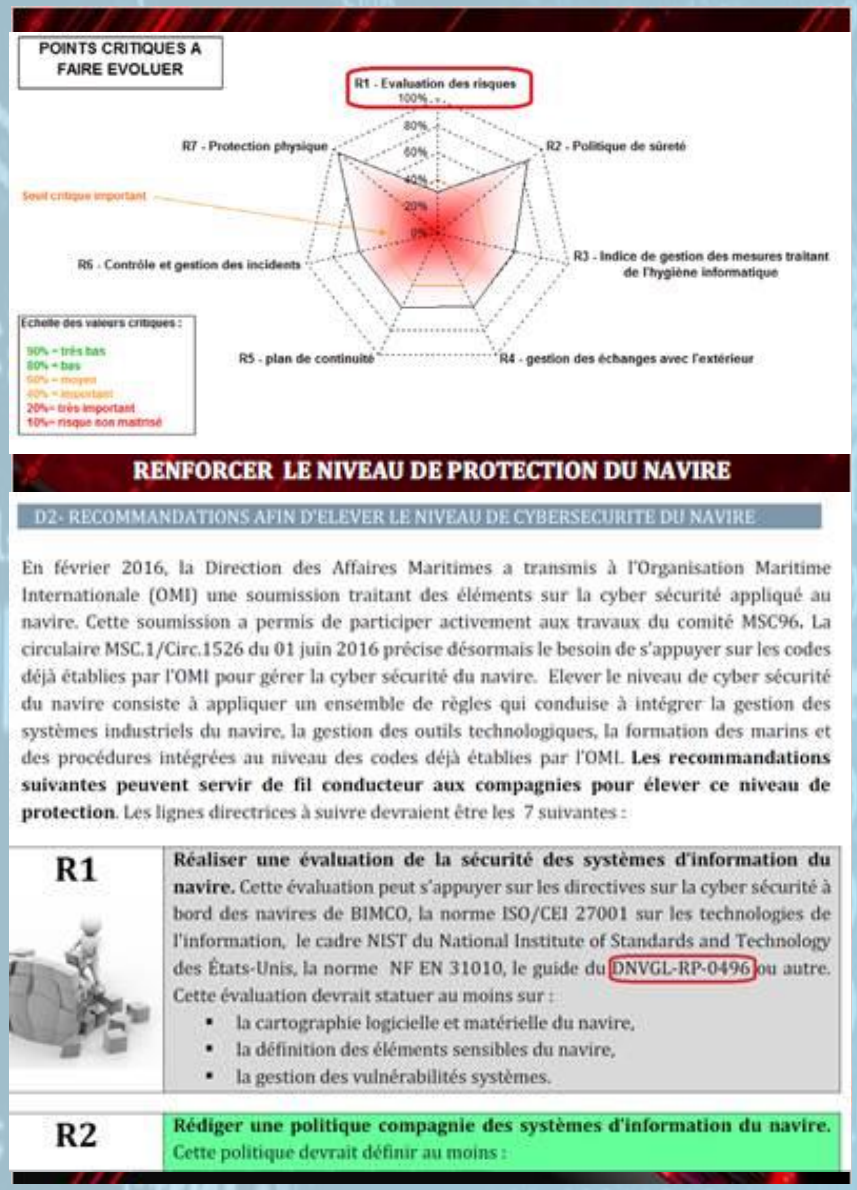
CYBER SECURITY DNVGL-RP-0496

"Looks really good, best CS guideline out there"
Passenger company

"We embrace this approach, thumbs up for the initiative"
Shipping manager

"This RP is absolutely useful in bridging the gap between the IT & OT* worlds"
Shipping manager

"Outstanding guidance that can be easily understood and embraced by most organizations"
Flag state



This RP is a comprehensive document that provides a good approach to Cyber Security for ICS*"
Shipping manager

"This RP makes a lot of sense"
Shipping manager

"Generally very good approach and description of the requirements"
Gov. agency

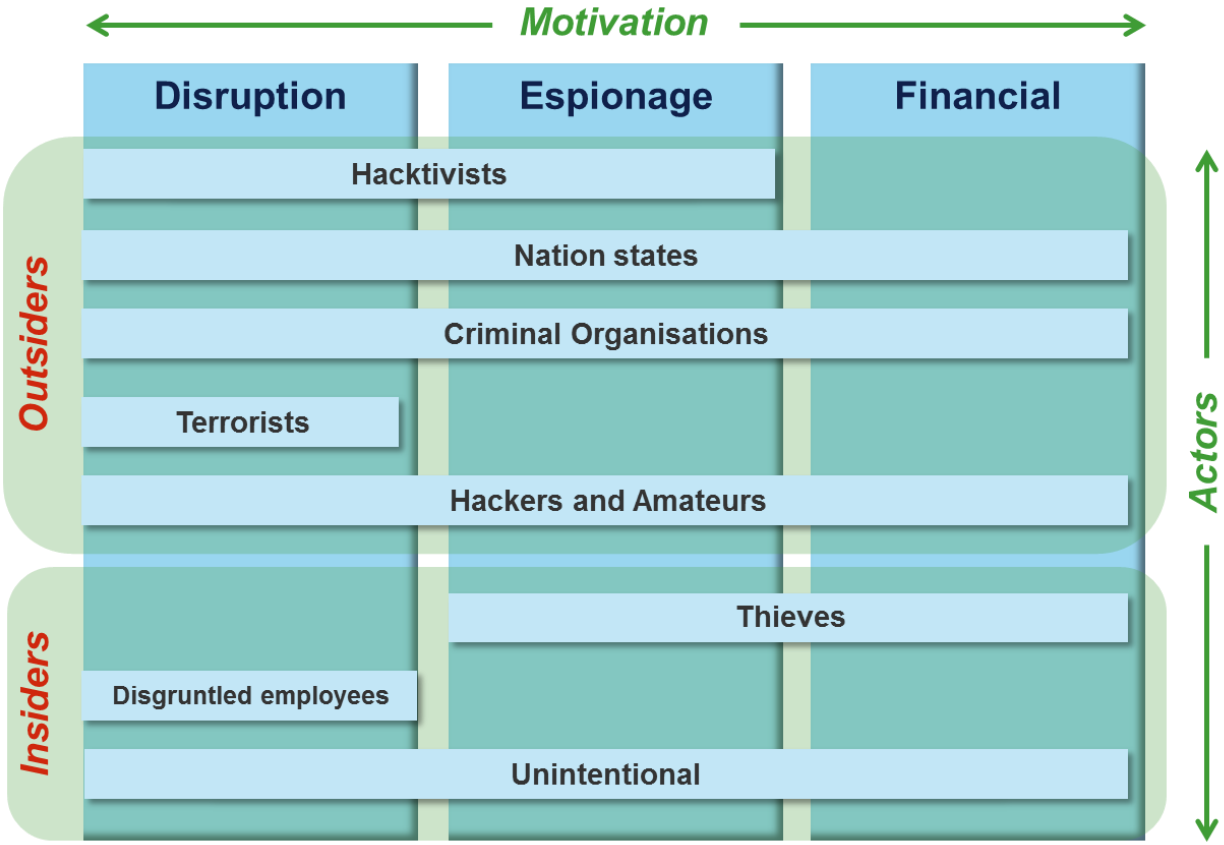
"Good overview of the recommended process with supporting tables, examples, checklists etc. Overall well done!"
Shipping manager

*OT: Operational Technology (Automation, Sensors, Industrial Control Systems (ICS)

Understanding Cyber Security threats/risks

- Threat Agents come in many flavours

Threat Agents



Understanding Cyber Security threats/risks

- Nuts & Bolts of a threat scenario :

Threat Agents

+

Motivation

+

Capability

Physical infrastructure

+ **Opportunity**
(overlap of Capability and knowledge of Physical infrastructure)

Understanding Cyber Security threats/risks

LIKELYHOOD <-?

- Identify critical systems
- Rank risks (prioritise)

Remote connection	Physically accessible	Connected and/or integrated	Requiring software updates	Ease of Access
X	-	-	-	Medium
X	-	-	X	High
X	-	X	No effect on Ease of access	High
X	X			High
-	-	X		Medium
-	X	-		Medium
-	X	X		Medium
X	X	X		High
-	-	-	X	Medium
-	-	-	-	Low

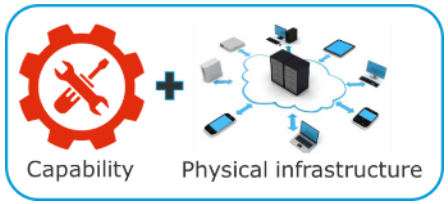
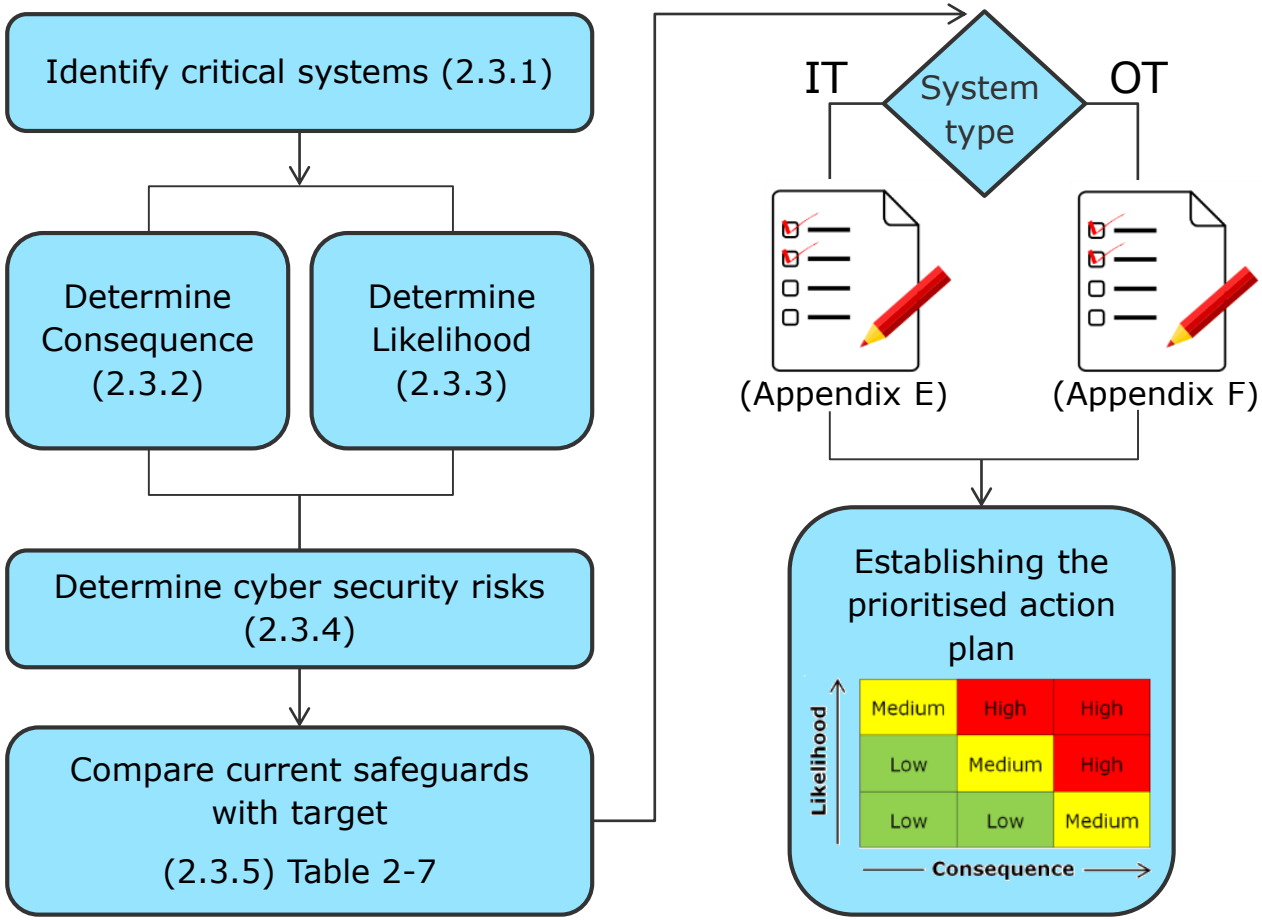


Table 2-4 Example rating of 'ease of access' (likelyhood)
DNVGL-RP-0496 - Cyber security resilience management for ships and mobile offshore units in operation

DNVGL-RP-0496: Comprehensive, in depth approach



Compare current safeguards with target

- Assessment results defines the target safeguards based on:

Module 5 - Applications	*Safeguard*	*Requirement*	*L*	*M*	*H*
S 5.2 Exchange of data media	S 3.14	Briefing personnel on correct procedures of exchanging data media		×	×
S 5.2 Exchange of data media	S 4.33	Use of a virus scanning program on exchange of data media and during data transfer	×	×	×
S 5.2 Exchange of data media	S 4.35	Pre-dispatch verification of the data to be transferred			×
S 5.3 Groupware	S 3.76	Basic user training on how to use groupware and e-mail			×
S 5.3 Groupware	S 4.199	Avoiding problematic file formats		×	×
S 5.3 Groupware	S 4.357	Secure operation of groupware systems	×	×	×
S 5.3 Groupware	S 4.358	Logging groupware systems		×	×
S 5.3 Groupware	S 5.54	Dealing with unwanted e-mails		×	×
S 5.3 Groupware	S 5.56	Secure operation of a mail server	×	×	×
S 5.3 Groupware	S 5.108	Cryptographic protection of groupware and/or e-mail			×
S 5.3 Groupware	S 5.109	Use of an e-mail scanner on the mail server			×
S 5.4 Web servers	S 2.174	Secure operation of a web server	×	×	×
S 5.4 Web servers	S 2.273	Prompt installation of security-relevant patches and updates	×	×	×
S 5.4 Web servers	S 4.33	Use of a virus scanning program on exchange of data media and during data transfer	×	×	×
S 5.4 Web servers	S 4.78	Careful modifications of configurations	×	×	×
S 5.4 Web servers	S 4.177	Assuring the integrity and authenticity of software packages		×	×
S 5.4 Web servers	S 5.59	Protection against DNS spoofing in authentication mechanisms	×	×	×
S 5.5 Lotus Notes/Domino	S 4.128	Secure operation of the Lotus Notes/Domino environment	×	×	×
S 5.5 Lotus Notes/Domino	S 4.132	Monitoring the Lotus Notes/Domino environment			×
S 5.5 Lotus Notes/Domino	S 4.426	Archiving for the Lotus Notes/Domino environment			×
S 5.5 Lotus Notes/Domino	S 4.427	Security-relevant logging and evaluating for Lotus Notes/Domino			×
S 5.5 Lotus Notes/Domino	S 4.428	Audit of the Lotus Notes/Domino environment			×
S 5.6 Fax servers	S 5.24	Use of a suitable fax cover sheet			×
S 5.6 Fax servers	S 5.25	Using transmission and reception logs	×	×	×
S 5.6 Fax servers	S 5.26	Announcing fax messages via telephone			×
S 5.6 Fax servers	S 5.27	Acknowledging successful fax reception via telephone			×

BSI GS

and

Table F-4 Requirements for Availability in OT system

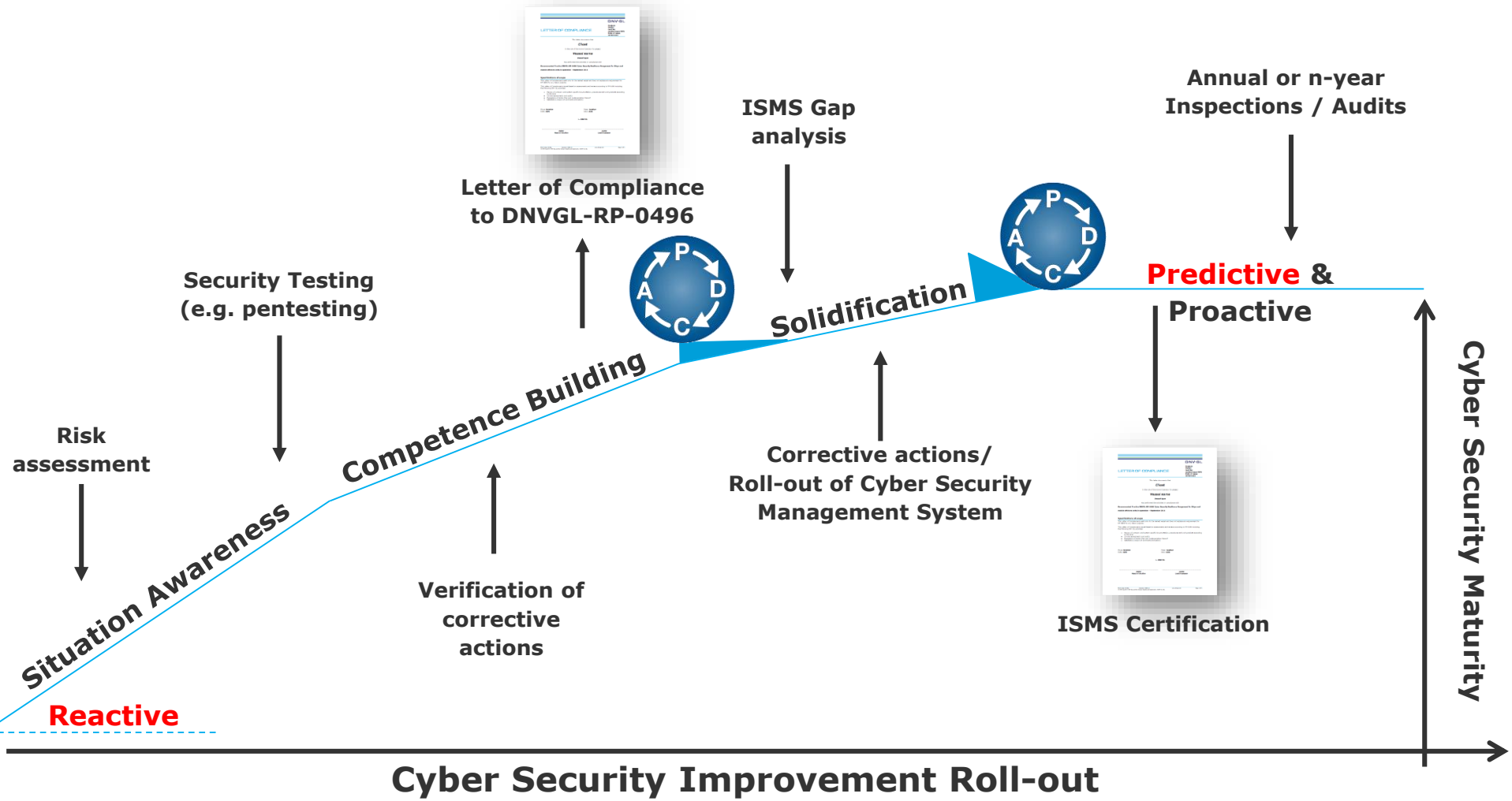
Availability	*Restricted data flow and timely response to events and resource availability*	*L*	*M*	*H*
SR 5.1	Network segmentation	×	×	×
SR 5.1 RE 1	Physical network segmentation	×	×	×
SR 5.1 RE 2	Independence from non-control system networks	×	×	×
SR 5.1 RE 3	Logical and physical isolation of critical networks	×	×	×
SR 5.2	Zone boundary protection	×	×	×
SR 5.2 RE 1	Deny by default, allow by exception		×	×
SR 5.2 RE 2	Island mode			×
SR 5.3	General purpose person-to-person communication restrictions	×	×	×
SR 5.3 RE 1	Prohibit all general purpose person-to-person communications	×	×	×
SR 5.4	Application partitioning	×	×	×
SR 7.1	Denial of service protection	×	×	×
SR 7.1 RE 1	Manage communication loads		×	×
SR 7.1 RE 2	Limit DoS effects to other systems or networks			×
SR 7.2	Resource management	×	×	×
SR 7.3	Control system back-up	×	×	×
SR 7.3 RE 1	Backup verification		×	×
SR 7.3 RE 2	Backup automation			×
SR 7.4	Control system recovery and reconstitution	×	×	×
SR 7.5	Emergency power		×	×
SR 7.6	Network and security configuration	×	×	×
SR 7.6 RE 1	Machine-readable reporting of current security settings			×
SR 7.7	Least functionality	×	×	×
SR 7.8	Control system component inventory		×	×

Table F-5 Requirements for Authenticity in OT system

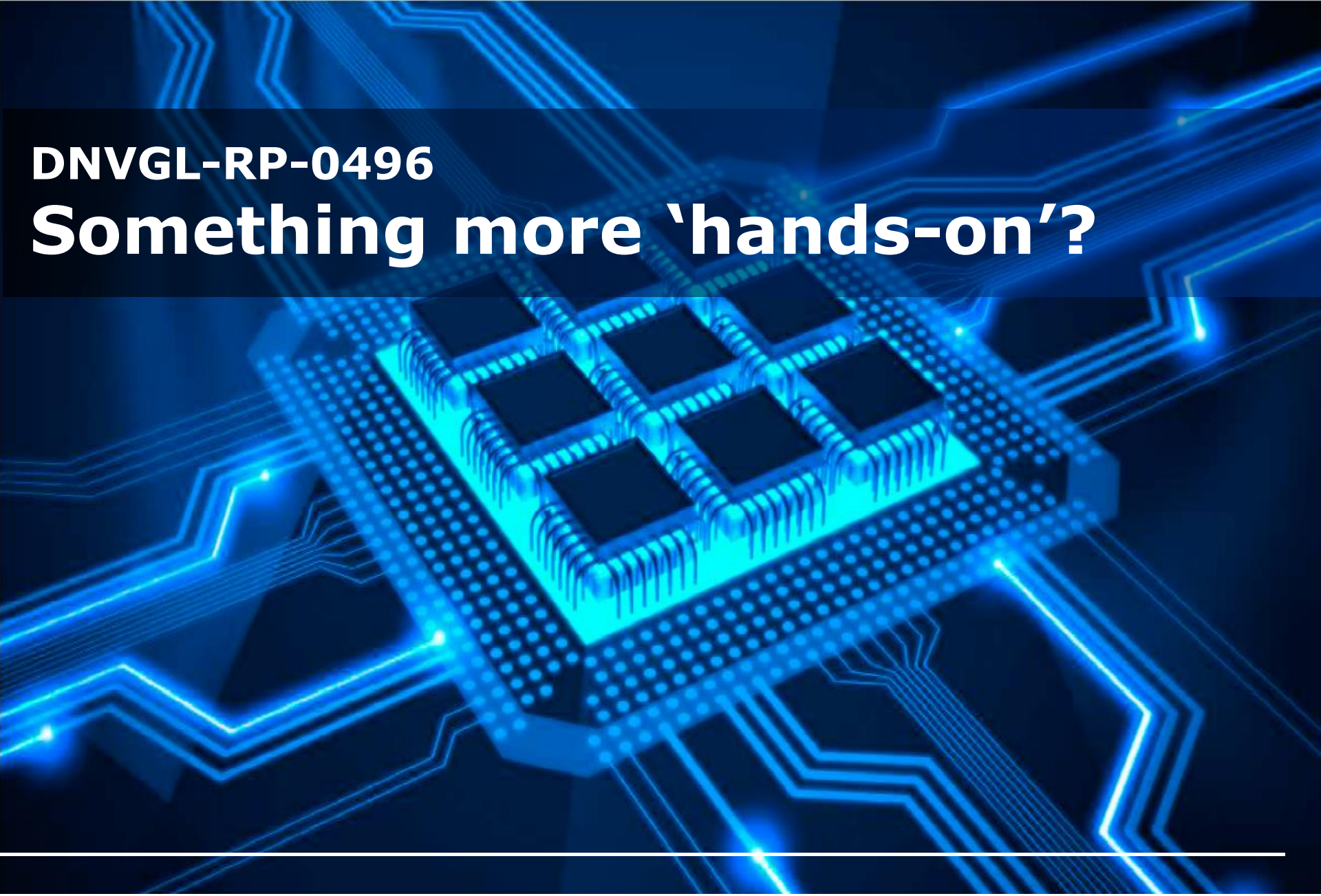
Authenticity	*Identification and authentication control and use control*	*L*	*M*	*H*
SR 1.1	Human user identification and authentication	×	×	×
SR 1.1 RE 1	Unique identification and authentication			×
SR 1.2	Software process and device identification and authentication		×	×
SR 1.3	Account management	×	×	×
SR 1.4	Identifier management	×	×	×

IEC 62443-3-3

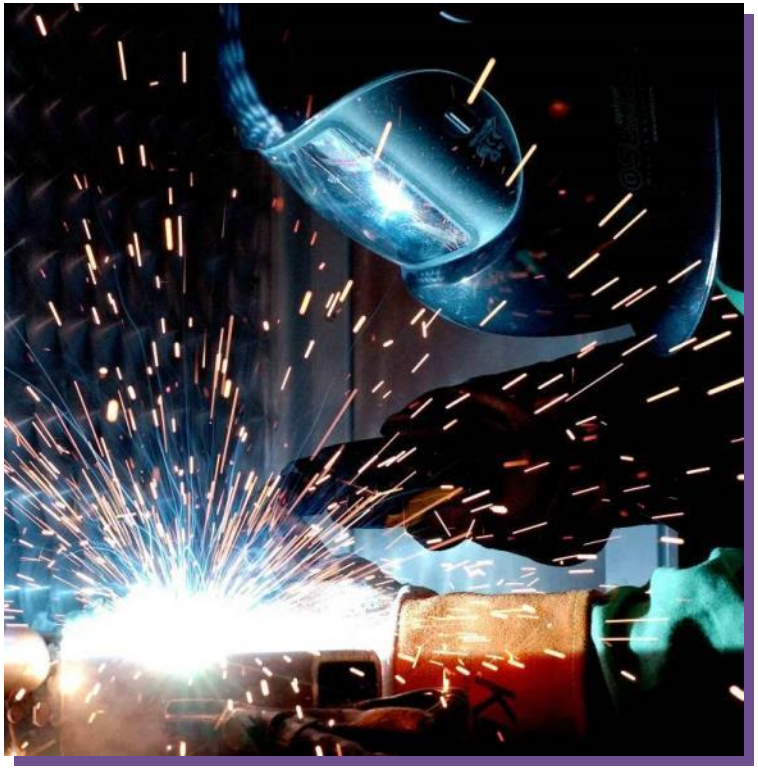
What to do during the lifecycle of a cyber-enabled vessel?

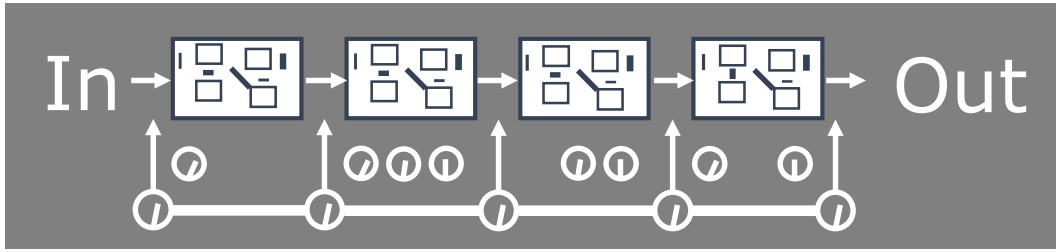


DNVGL-RP-0496
Something more ‘hands-on’?

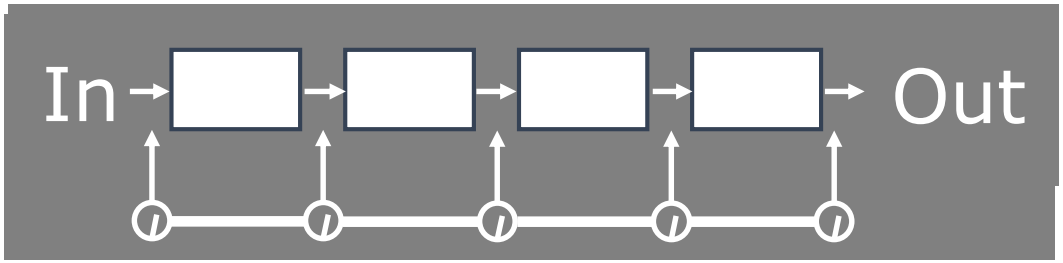


When welding/repair, a 'crack' is introduced to the vessel structure – how is this crack (risk) controlled?





When software change is introduced to systems - then what?



Bridging the Physical and the Cyber domains

Physical		Cyber physical
Risk assessment	→	Threat analysis
Fire drills	→	System restore drills
Permit to work	→	SW Change management
Drawings	→	Software topology, CMDB
Changing slowly	→	Changing fast
Easy to test	→	Difficult to test

Bridging the Physical and the Cyber domains

Physical

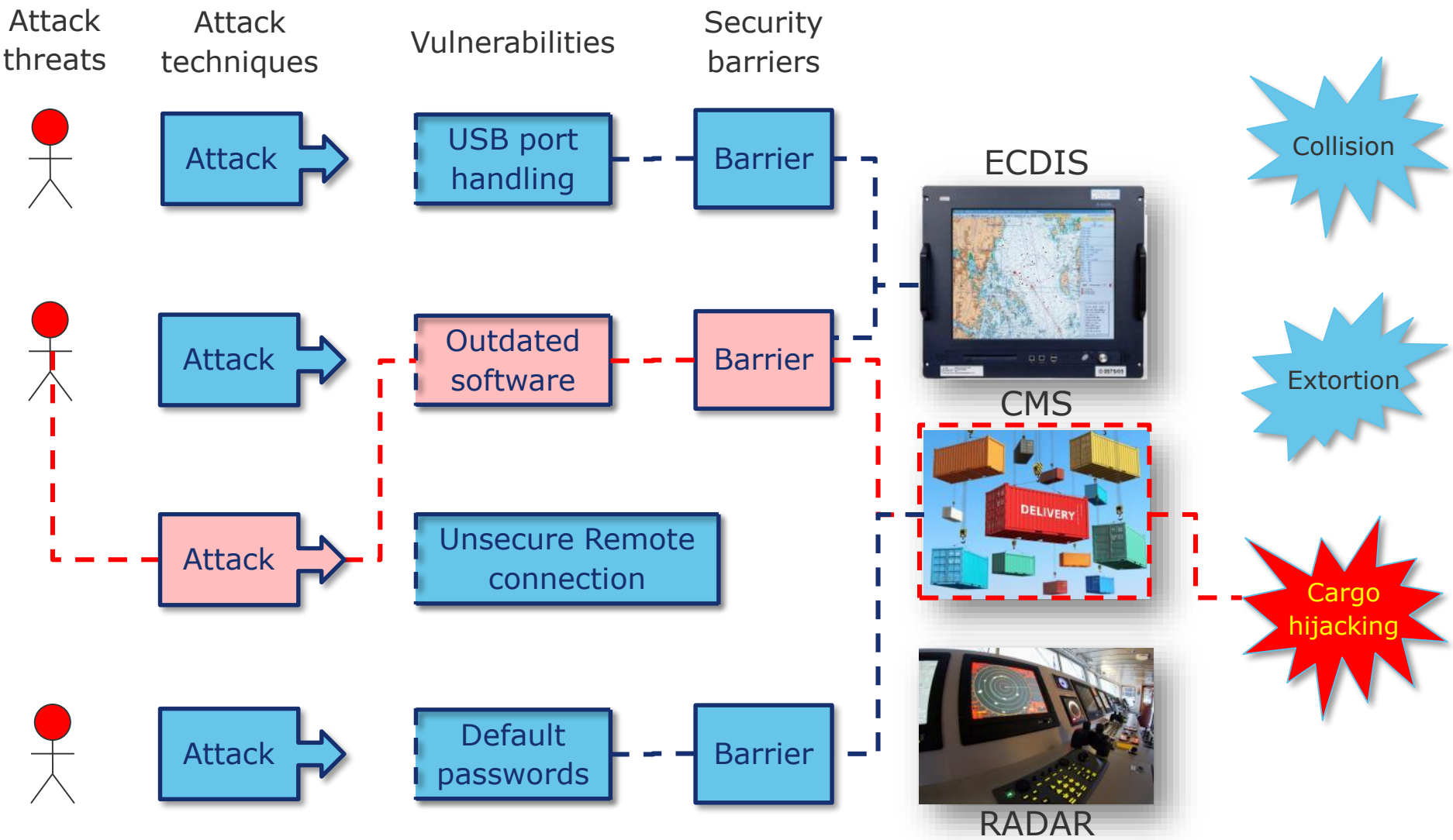
- Risk assessment
- Fire drills
- Permit to work
- Drawings
- Changing slowly
- Easy to test

Software has to be tracked as a component just like it's done in the physical world

Cyber physical

- Threat analysis
- System restore drills
- SW Change management
- Software topology, CMDB
- Changing fast
- Difficult to test

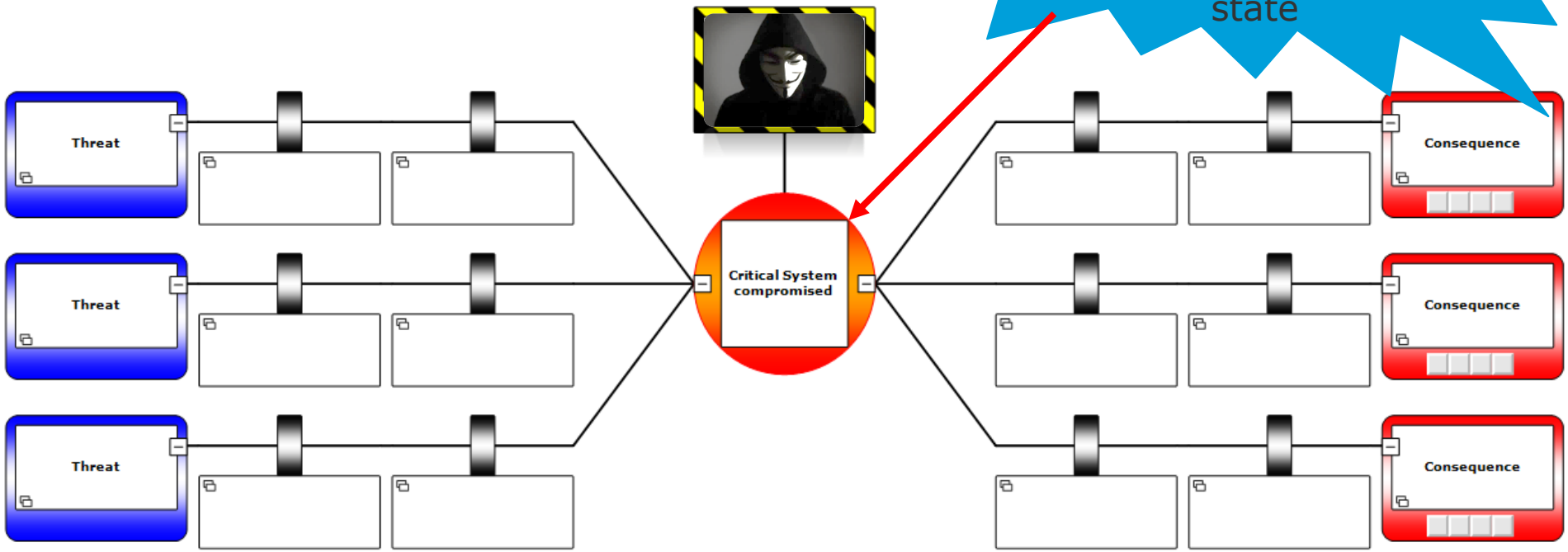
Understanding cyber attack mechanics: Attacker → Vulnerabilities → Barriers → Consequences



DNVGL-RP-0496: Graphical understanding of protection barriers

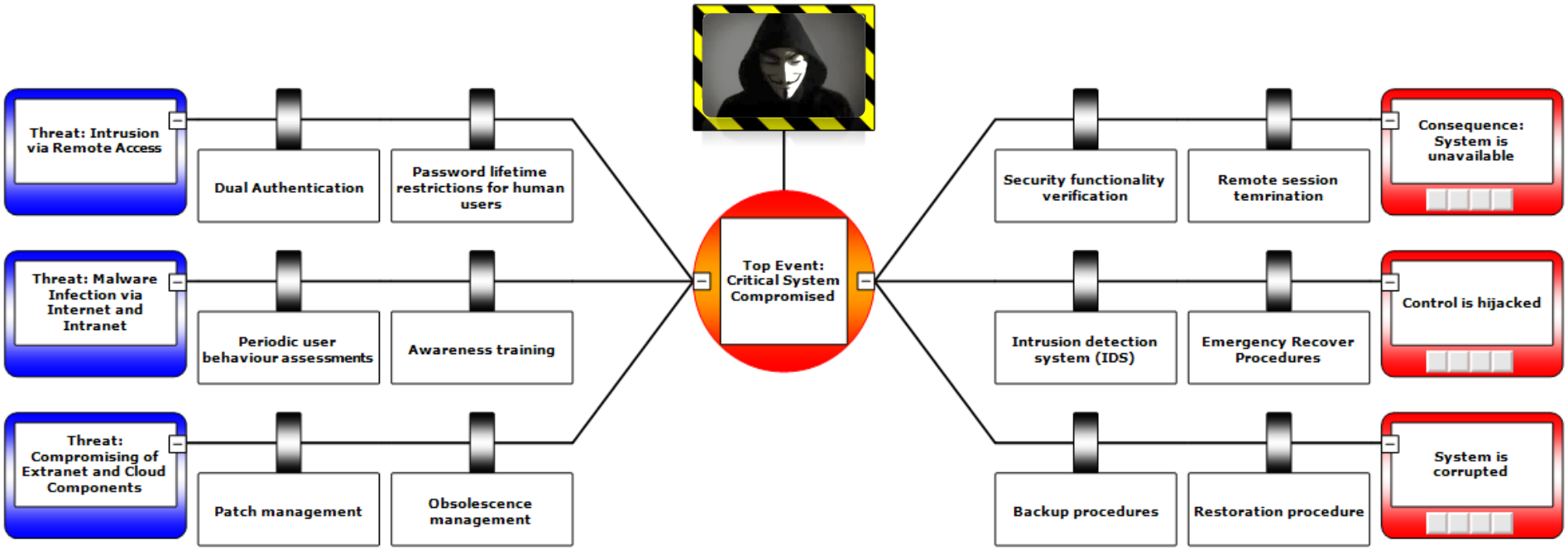
- 2.2.2. Identify threats and consequences
- 2.2.3. Identify incident prevention barriers
- 2.2.4. Identify consequence reduction barriers

First start by defining the undesirable event, i.e. which specific system and unwanted state



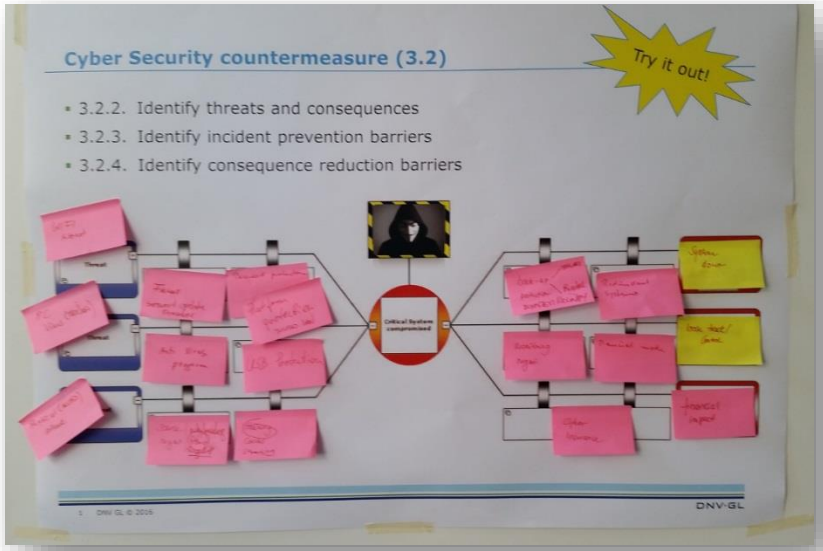
DNVGL-RP-0496: Graphical understanding of protection barriers

- Leverages existing industry knowledge using Bow-Tie & Barrier management methodologies and transposes this intuitive method to help assess complex attack scenarios



A bridge between domain knowledge

- Use graphical tools for communication with industry language
- Bow-tie barrier management ⇔ Safety

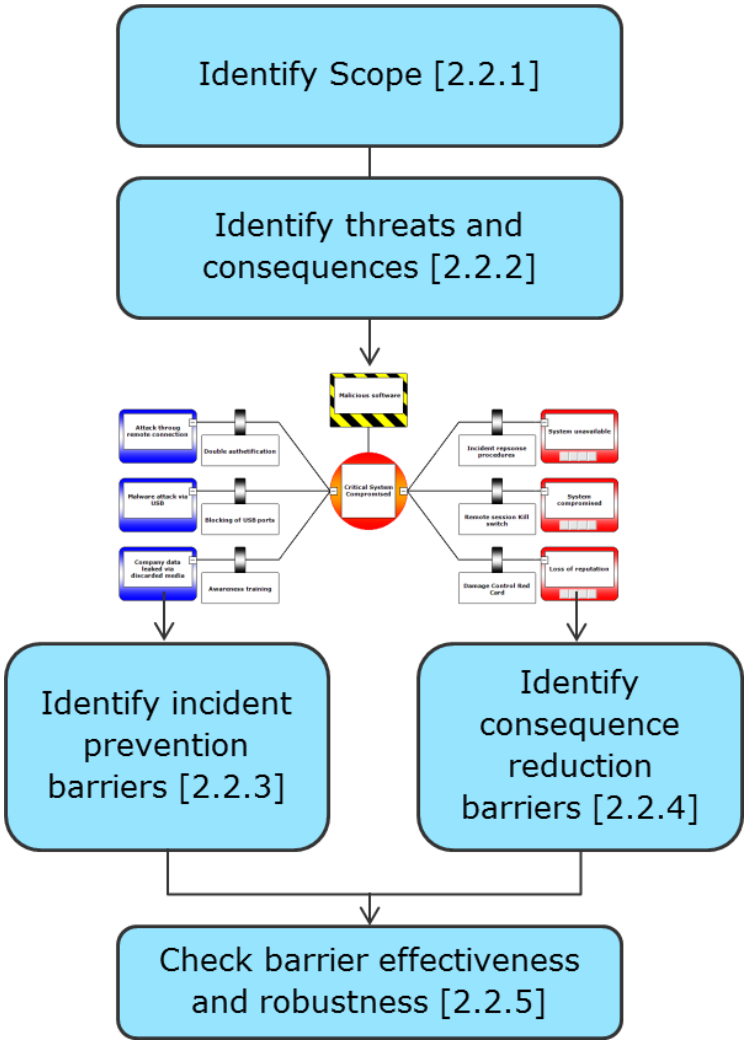


Non IT background people learn how to do it in 10 minutes and realise they know a lot more than they thought

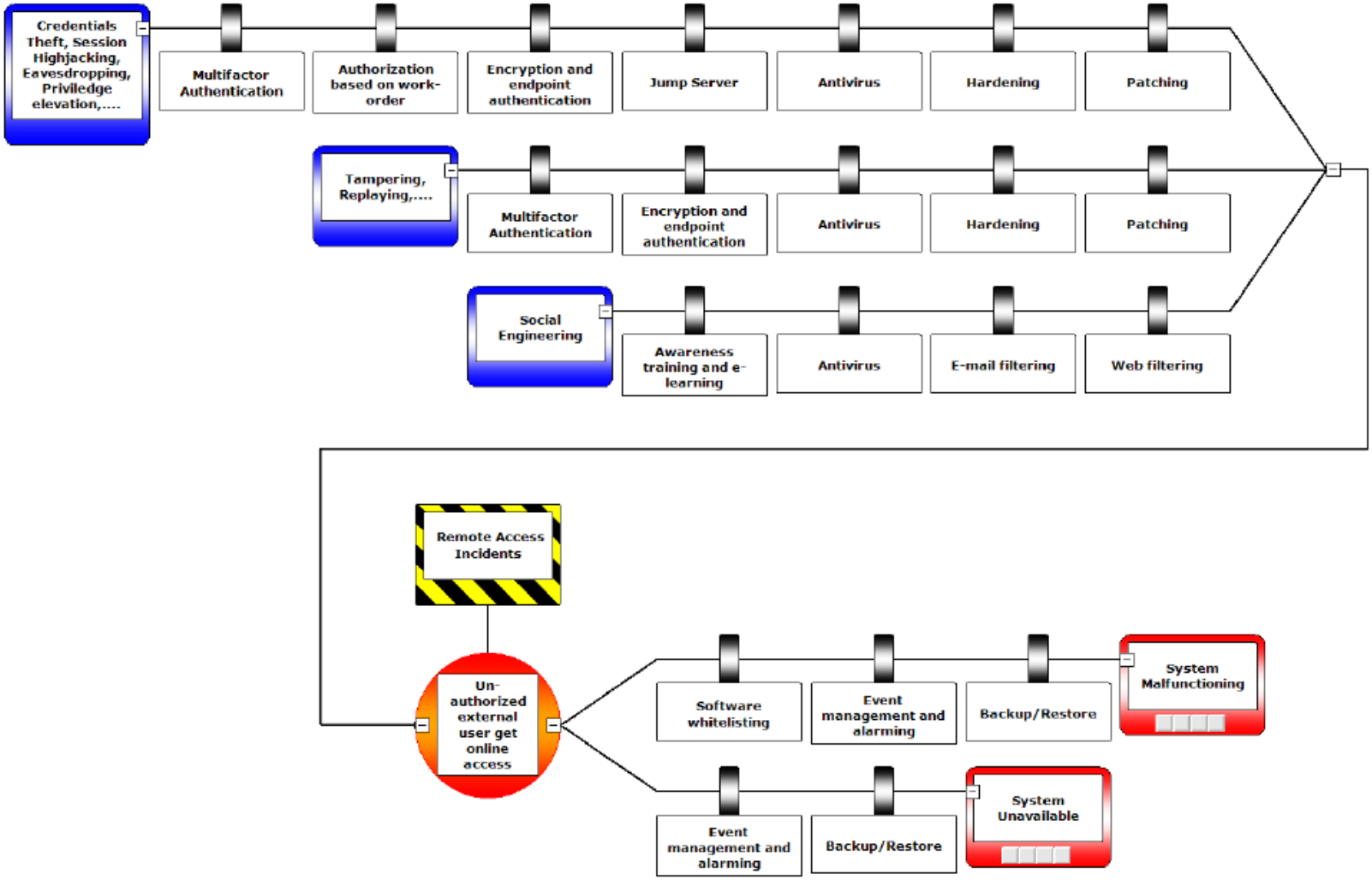
DNVGL-RP-0496: Graphical understanding of protection barriers

- Cyber Security Bow-Tie barrier management methodology leverages existing industry knowledge and transposes this intuitive method to help assess complex attack scenarios

- Referencing recognised guidance such as DNVGL-RP-0496 §2.2 or §2.3 in company procedures is a sound approach



Bow-tie example Remote connections (e.g. for Remote maint.)



Solutions

The TMSA3 Cyber KPIs

Market demand for more consideration of cyber risks

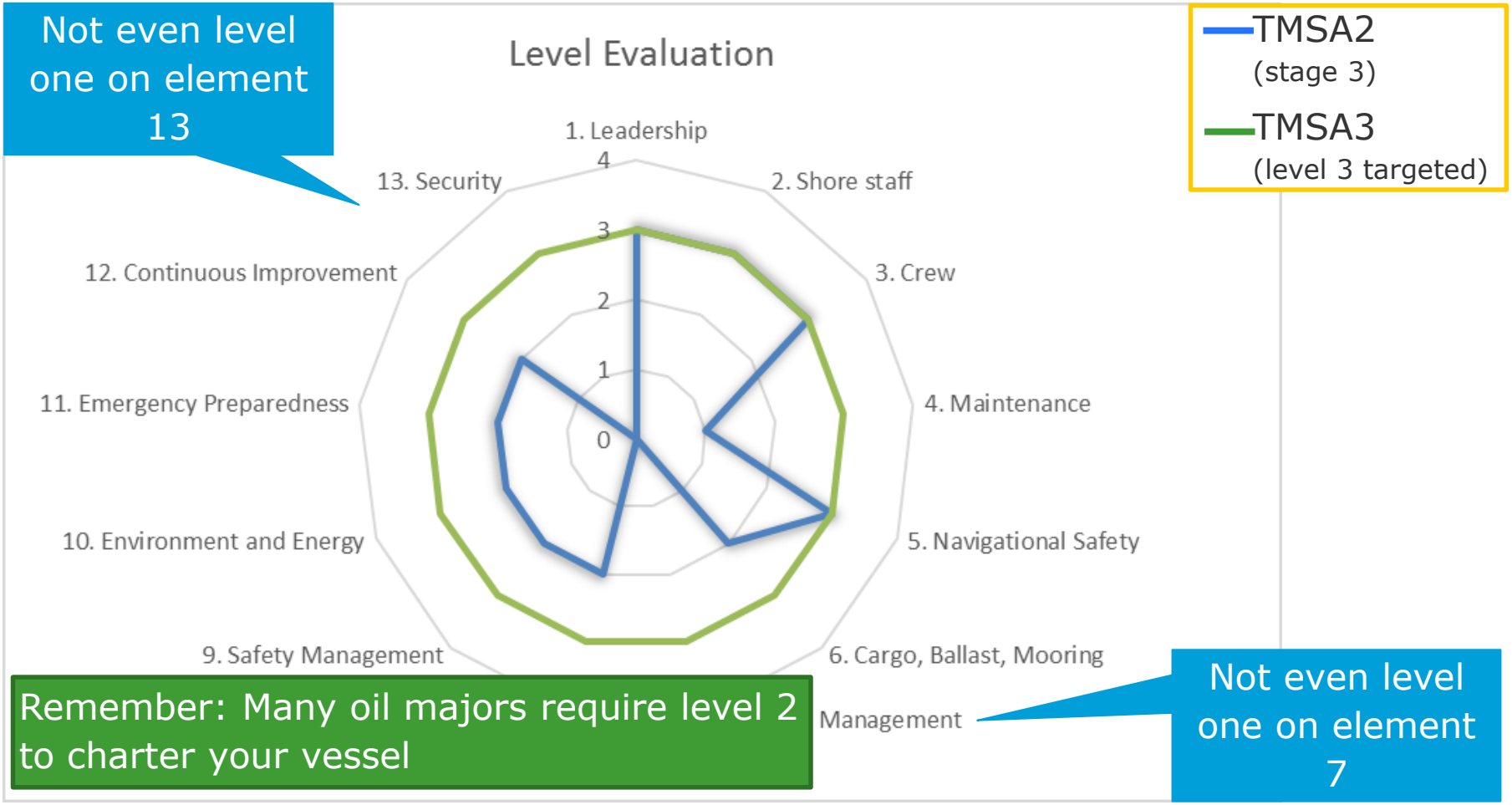
- Tanker Management and Self Assessment (TMSA) No. 3, published in April 2017.
  - Includes two new cyber security related chapters
    - Element 7 – Management of Change
    - Element 13 – Maritime Security
  - KPIs and 3rd party audits, e.g.:
    - Software management procedure covers all shipboard and shore systems
    - Actively promoting cyber security awareness
    - Policy and procedures include cyber security
  - **Charters** demand TSMA audits of ships.
  - TMSA 3 to be met by **1st Jan. 2018**

TMSA3 – 13 elements

Element	Title
1	**Leadership** and the Safety Management System
2	Recruitment and Management of **Shore-Based Personnel**
3	Recruitment, Management and Wellbeing of **Vessel Personnel**
4	Vessel **Reliability and Maintenance** including Critical Equipment
5	**Navigational Safety**
6	**Cargo**, Ballast, Tank Cleaning, Bunkering, **Mooring and Anchoring** Operations
7	Management of **Change**
8	**Incident** Reporting, Investigation and Analysis
9	**Safety Management**
10	**Environmental and Energy** Management
11	**Emergency Preparedness** and Contingency Planning
12	**Measurement**, Analysis and **Improvement**
13	Maritime **Security**

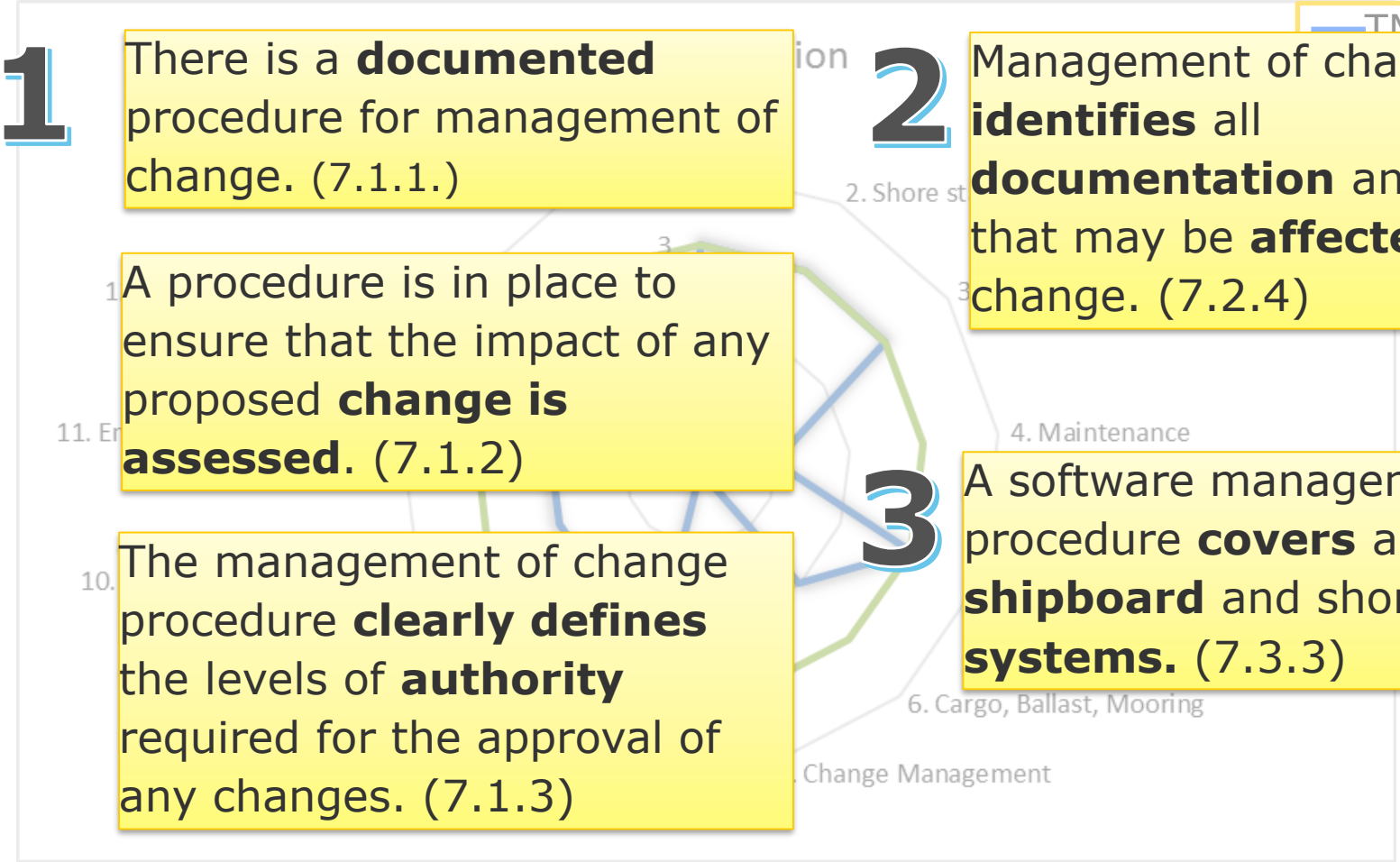
New!

What happens when you move to TMSA3 – including the new Cyber Security KPIs?



Example: TMSA2 Stage 3 company has "yes" on all TMSA3 KPIs up to Level 2. "No" on all new TMSA3 KPIs at levels 3 and 4 **and on all Cyber/Software KPIs.**

5 Cyber Security KPIs in Element 7 – Management of Change



1 There is a **documented** procedure for management of change. (7.1.1.)

2 Management of change **identifies** all **documentation** and records that may be **affected** by the change. (7.2.4)

A procedure is in place to ensure that the impact of any proposed **change is assessed**. (7.1.2)

3 A software management procedure **covers** all **shipboard** and shore **systems.** (7.3.3)

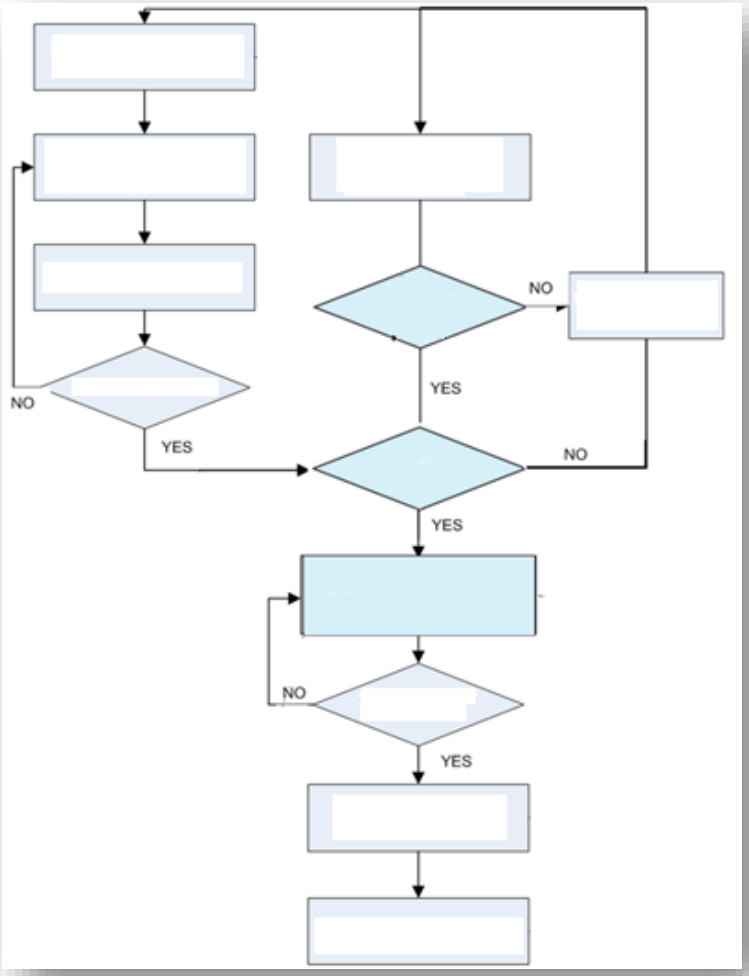
The management of change procedure **clearly defines** the levels of **authority** required for the approval of any changes. (7.1.3)

Software configuration control workflow

- Software changes must be planned and recorded. Example:
  - Software update (Windows, Patch)
  - Firmware update
  - Supplier adds/remove functionality
  - Bug fix, upgrades

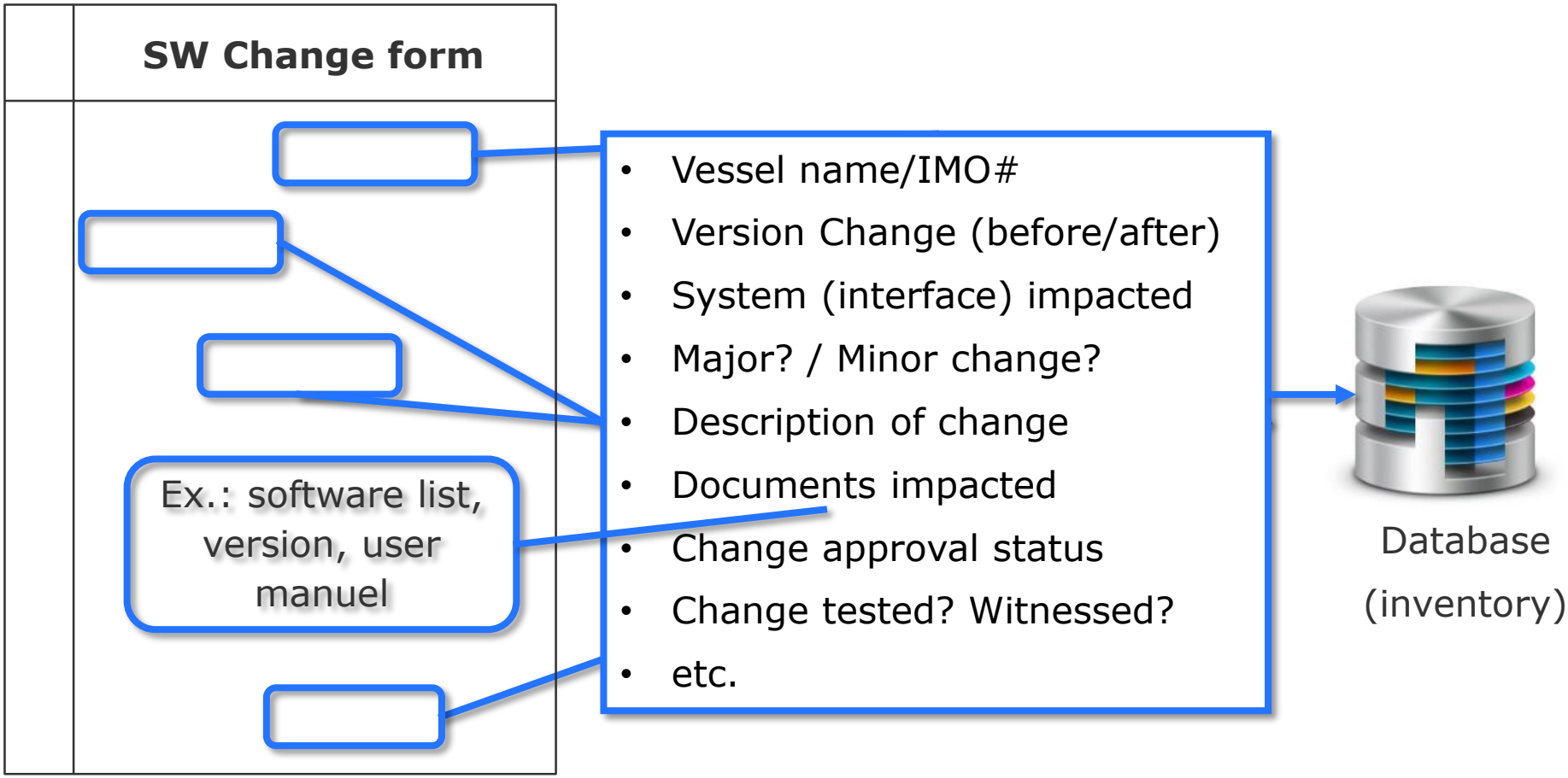
- Software changes should be categorised as major or minor changes

- Major changes must be submitted to Configuration Control Board (CCB) for approval/witnessing



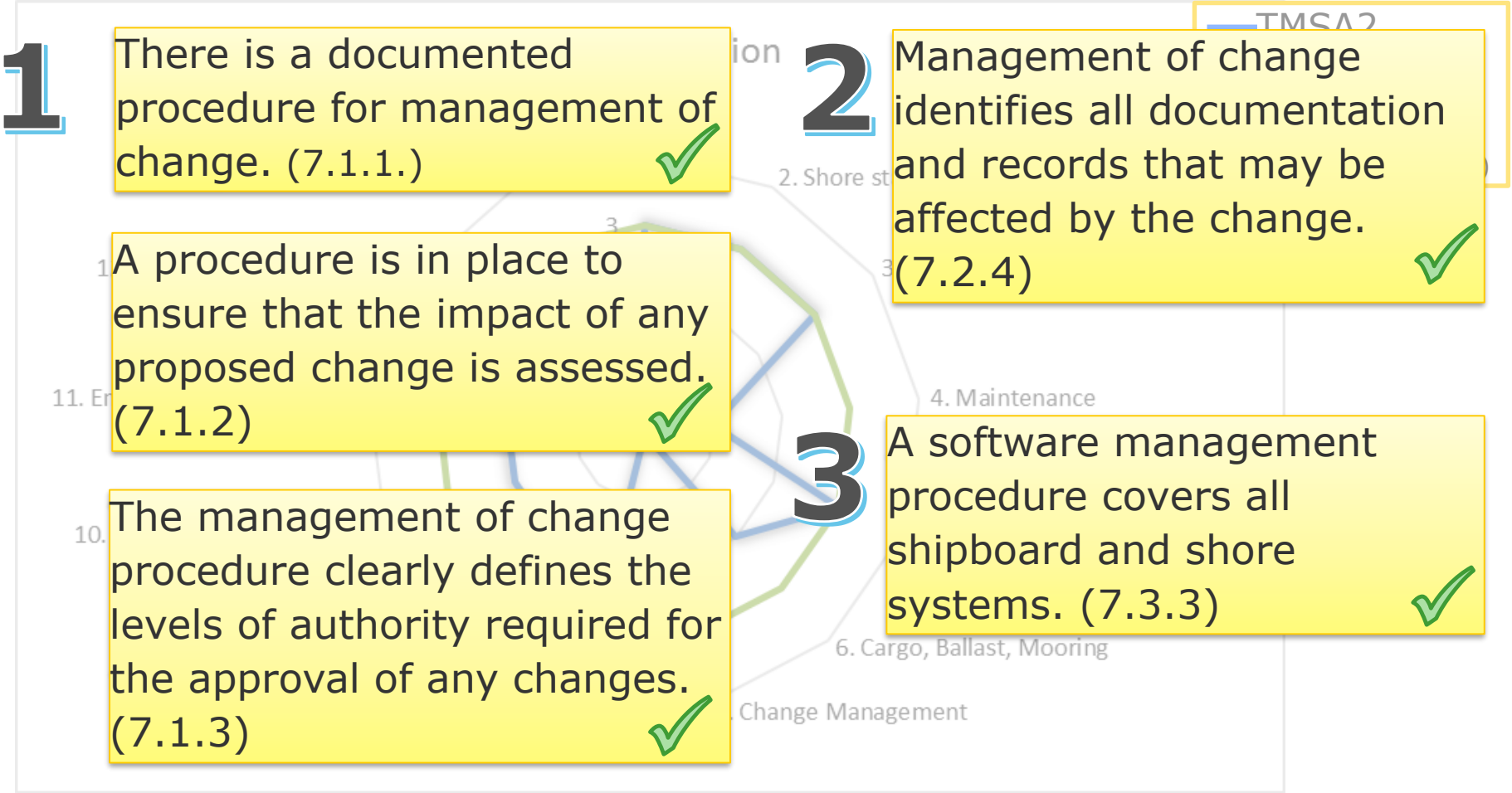
Same as for hot work: SW changes should be approved

SW configuration/change tracking system



Same as for hot work: SW change form should be required

5 Cyber Security KPIs in Element 7 – Management of Change



1 There is a documented procedure for management of change. (7.1.1.)

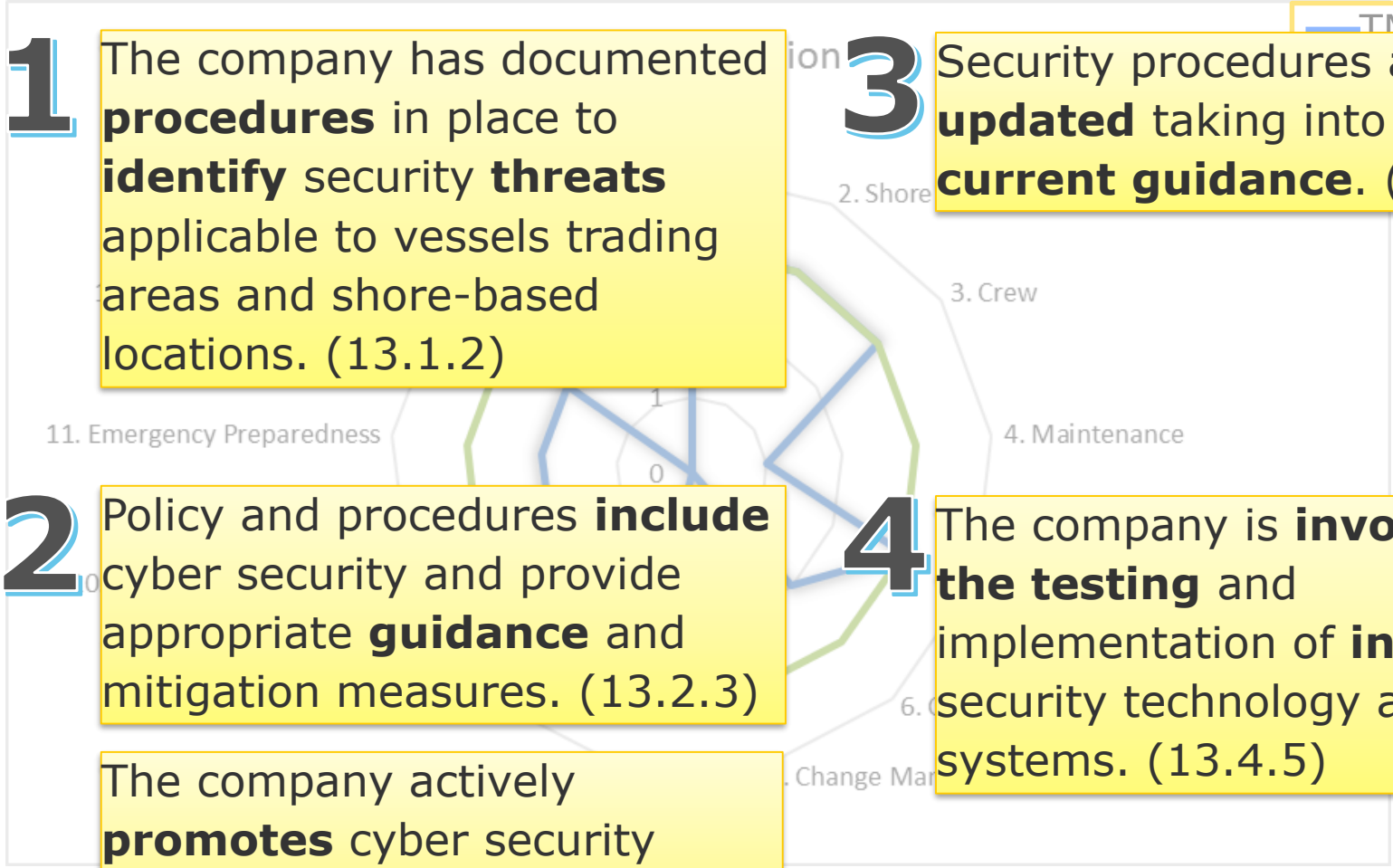
A procedure is in place to ensure that the impact of any proposed change is assessed. (7.1.2)

The management of change procedure clearly defines the levels of authority required for the approval of any changes. (7.1.3)

2 Management of change identifies all documentation and records that may be affected by the change. (7.2.4)

3 A software management procedure covers all shipboard and shore systems. (7.3.3)

5 Cyber Security KPIs in Element 13 – Maritime Security



1 The company has documented **procedures** in place to **identify** security **threats** applicable to vessels trading areas and shore-based locations. (13.1.2)

2 Policy and procedures **include** cyber security and provide appropriate **guidance** and mitigation measures. (13.2.3)

The company actively **promotes** cyber security **awareness**. (13.2.4)

3 Security procedures are **updated** taking into account **current guidance**. (13.3.2)

4 The company is **involved in the testing** and implementation of **innovative** security technology and systems. (13.4.5)

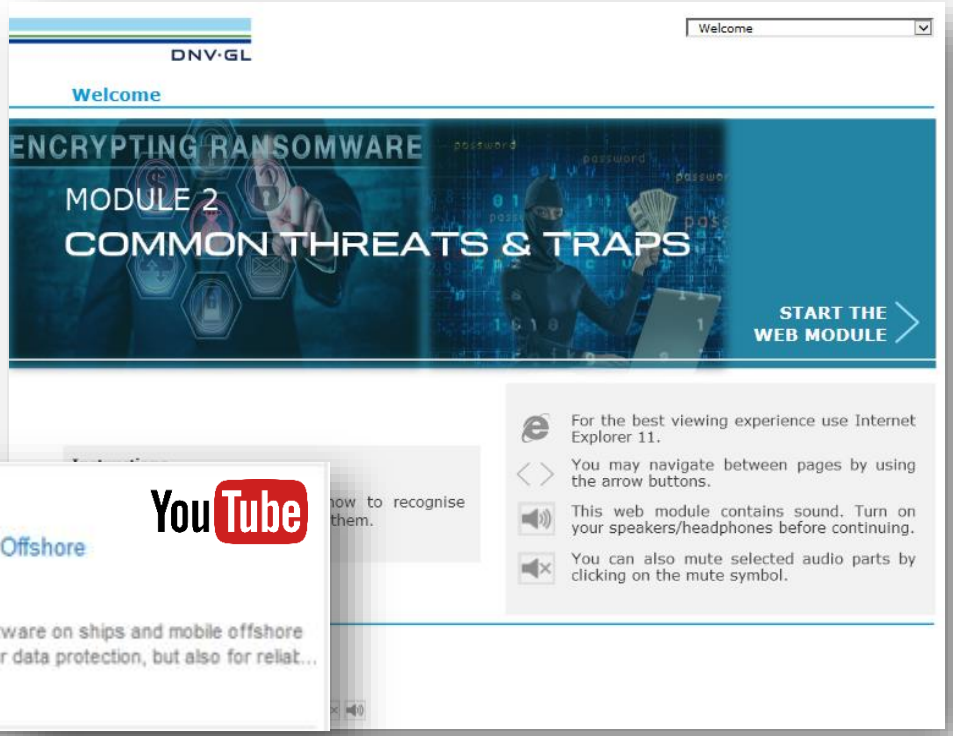
Use Cyber Security e-learning on shore or in transit

Promoting Cyber Security awareness is easy through e-learning

- Module 1: How you can help protect yourself and your organisation (10min)
- Module 2: Common threats & traps (15min)
- Module 3: Best practices (15min)
- Module 4 : Advanced defence in depth course (20min)

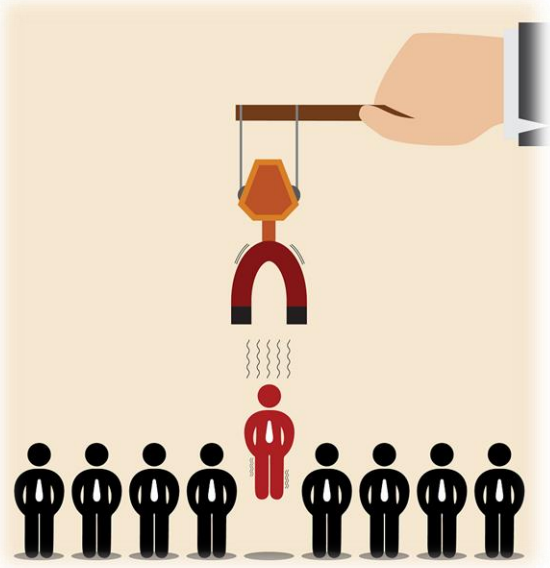
Available through our on board solution distributor

Seagull



Cyber Organised Crime starts with Social Engineering

- Remember the Nigerian prince scam?
- Now + more sophisticated:
  - Systematic decomposition and in depth understanding of Emotional Triggers



Understand the Cyber Security threats and Cyber-attack techniques

Precious information can be used by attackers who will then impersonate someone in close contact with your entourage or being a colleague from the same employer as you, or by advertising false job offers to trick you into an interview to gain more access to sensitive information.

Social network platforms therefore contain a gold mine of useful information for attackers looking for easy prey.

Cyber Organised Crime*

Boss

Underboss:
Trojan provider and Manager of Trojan
Command and Control

Attackers Crimeware Toolkit Owners
Trojan Distribution in Legitimate website

Campaign Manager

Campaign Manager

Campaign Manager

Affiliation Network

Affiliation Network

Affiliation Network

Stolen Data Reseller

Stolen Data Reseller

Stolen Data Reseller

source: EC-Council

***more organised than some governmental agencies…**

Saudi Aramco case

The hackers were never identified or caught (that we know of)

On the morning of Wednesday, Aug. 15, 2012, files began to disappear, computers started shutting down. No more Internet, corporate email or office phones. Lengthy, lucrative deals needing signatures **had to be faxed one page at a time…**
Temporarily stopped selling oil to domestic gas tank trucks and **after 17 days Saudi Aramco relented and started giving oil away for free to keep it flowing within Saudi Arabia…**
Representatives flew directly to computer factory floors in Southeast Asia to **purchase every computer hard drive being manufactured (50,000 hard drives)…**
Everyone who bought a computer or hard drive from September 2012 to January 2013 had to pay a slightly higher price for their hard drive…

Supply specifically designed Trojan Toolkit

Mid-2012, One of the computer technicians on Saudi Aramco's information technology team opened a scam email and clicked on a bad link. The hackers were in

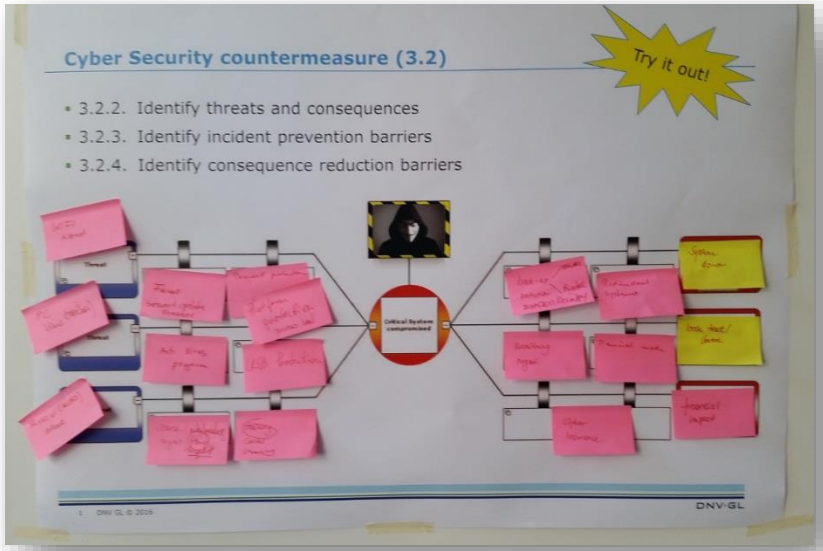
Who's interested in a Saudi Aramco breach (*9.5 million barrels per day production…*)?

Social engineering: Gaining understanding of emotional triggers


YOU
ARE
HERE

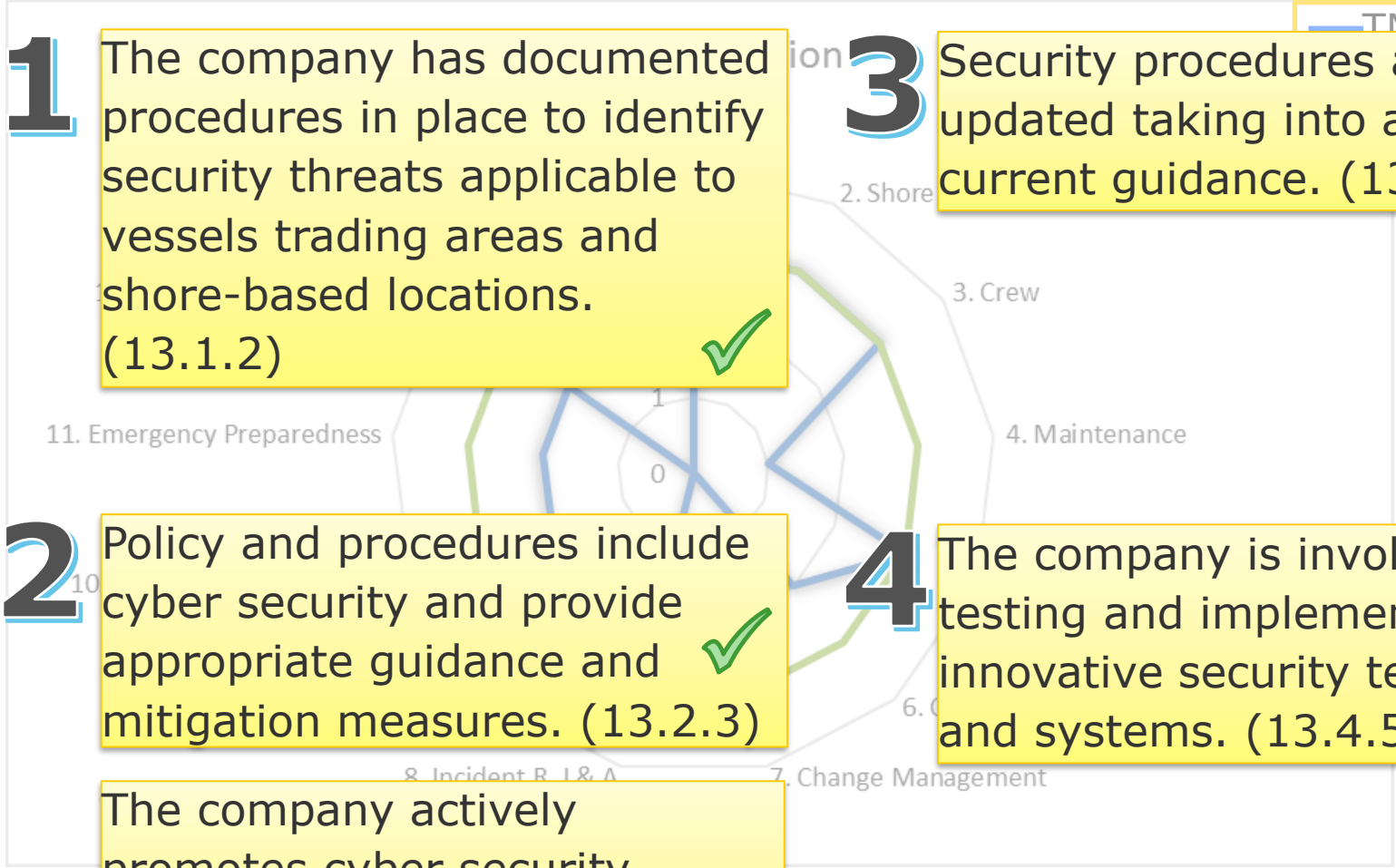
A bridge between domain knowledge (Recall)

- Use graphical tools for communication with industry language
- Bow-tie barrier management ⇔ Safety



Non IT background people learn how to do it in 10 minutes and realise they know a lot more than they thought

5 Cyber Security KPIs in Element 13 – Maritime Security



1 The company has documented procedures in place to identify security threats applicable to vessels trading areas and shore-based locations. (13.1.2)

2 Policy and procedures include cyber security and provide appropriate guidance and mitigation measures. (13.2.3)

The company actively promotes cyber security awareness. (13.2.4)

3 Security procedures are updated taking into account current guidance. (13.3.2)

4 The company is involved in the testing and implementation of innovative security technology and systems. (13.4.5)

On board Cyber Security inspections

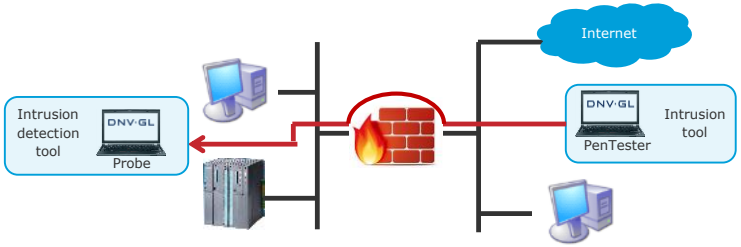
Interviews and spot checking (comparing the current safeguards with target protection levels):

- against policy, procedures, responsibilities and competence
- existence of controls and barriers

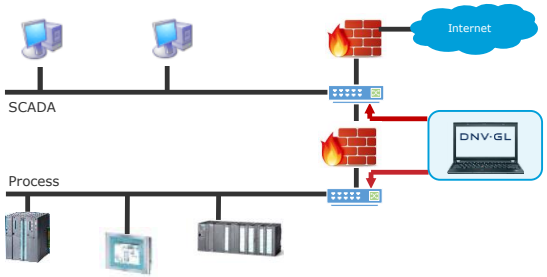
Vulnerability testing, spot-checking of most critical IT/OT systems using white/grey box testing

Verification & Validation by 3rd party Cyber Security testing

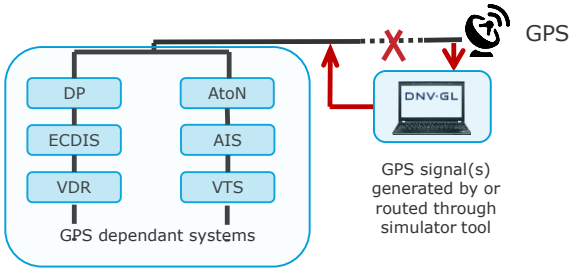
- Barrier testing tools & techniques of simulated hacking



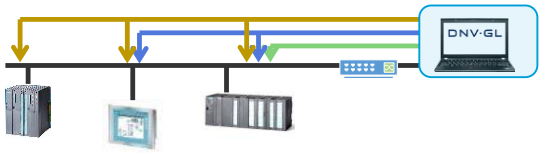
Penetration testing



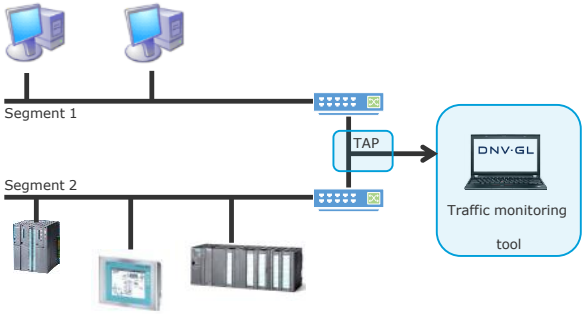
Vulnerability Scanning/Hacker Simulation



GPS Spoofing/Jamming Simulation



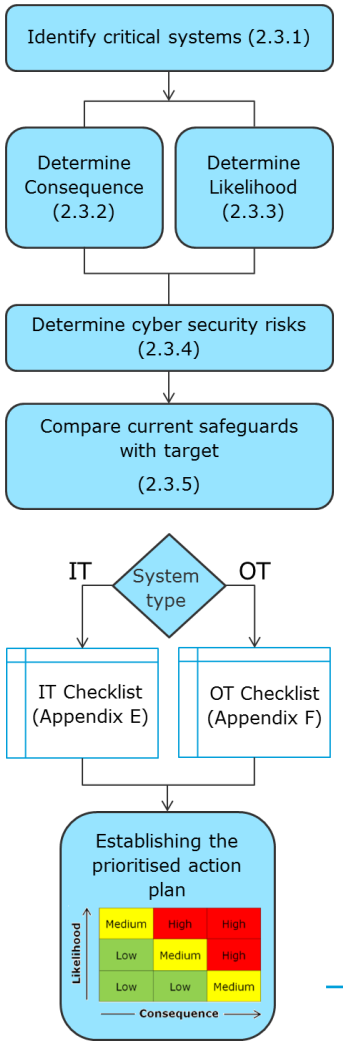
Network Storm & Stress testing



Passive Network Analysis

IoT Fuzz testing; Finding known and unknown (fuzzing) vulnerabilities

Activities towards Statement of Compliance with DNVGL-RP-0496



- Assessment workshop
- Building of check-lists
- 1st On board inspection
- Establish and review action plan
- Implementation of improvements
- 2nd On board inspection
- Issuing of Letter of Compliance

Simple steps and activities

- Systematically **change default settings** when installing new equipment
- **Practice** cyber incident **drills** (and keep records of it)
- **Control** the use of **removable media** (e.g. use USB port management systems)
- Have a **workshop** to discuss the risks **with your crew**
- Add Cyber on **board meeting agendas**
- Define **how vendors** should **interact** with your cyber related processes
- **Check effectiveness** of your cyber security (especially on critical functions)

Take aways

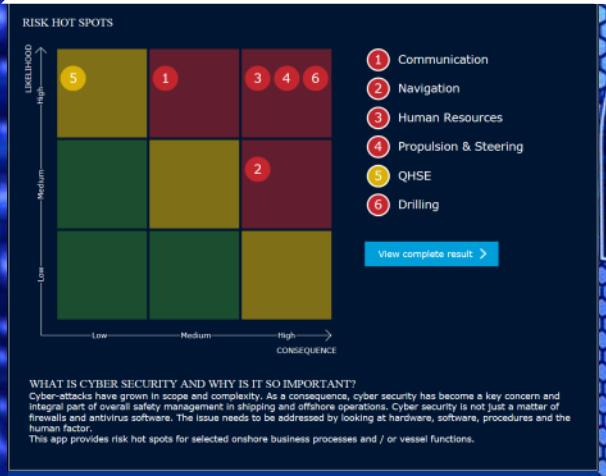
- **Start Small: Highlight sensate inventory**

- **You know more than you think: Everyone can play**

- **Ask questions: Your vendors and integrators will appreciate your interest**

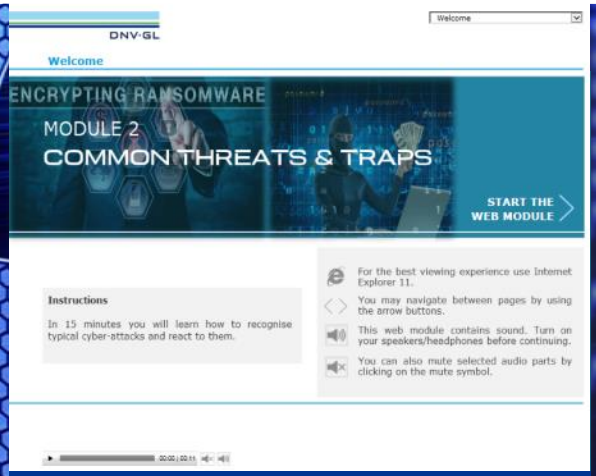
CYBER SECURITY
DNV GL's Recommended Practice… and related services

Assess



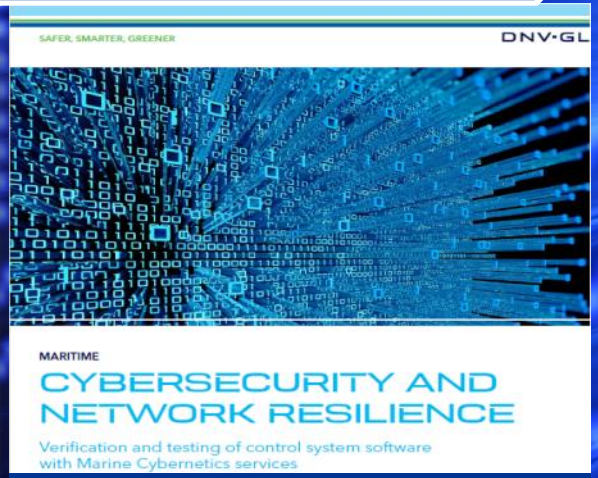
- **Self-assessment app in My DNV GL**
- **On-board inspections**
- **Focused risk assessment**
- **In-depth risk assessment**
- **Gap assessment for ISMS, GDPR and TMSA3+Cyber**

Improve



- **E-Learning modules [1-4]**
- **Class room training [1-3]**
- **Cyber security enhancement advisory**
- **Preparation for ISMS certification and GDPR/TMSA3+Cyber compliance**

Verify



- **Cyber Security testing**
- **Type approval of systems and components**
- **ISO/IEC 27001 certification**
- **GDPR & TMSA3+Cyber Statement of Confidence**
- **Verification of new build projects and Statement of Compliance acc. to DNVGL-RP-0496**

Thank you for your attention

Maritime Cyber security Download the RP free of charge from: www.dnvgl.com/rpcs

DNV GL MARITIME ADVISORY
patrick.rossi@dnvgl.com +49(0)151-67643274

CEH Certified Ethical Hacker