CYBER SECURITY AWARENESS IN THE MARITIME INDUSTRY

A joint production by DNV GL and GARD

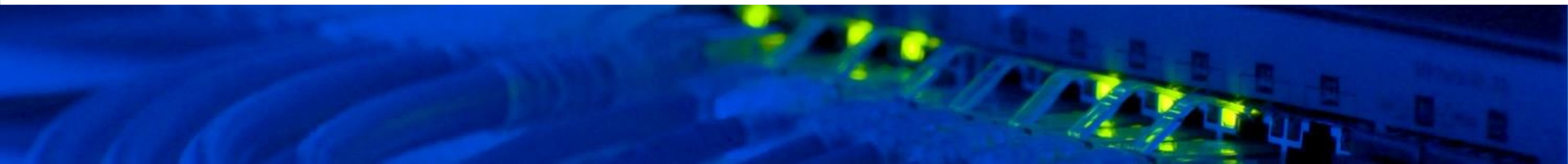
STRUCTURE

STATUS ON CYBER SECURITY IN MARITIME SHIPPING

Risk scenarios (threats)

Best practices for you and your company

DNV GL and Gard and cyber security

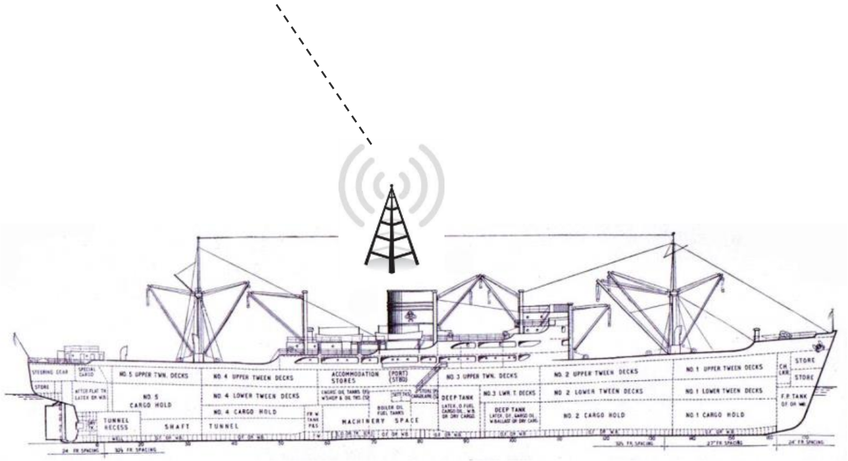


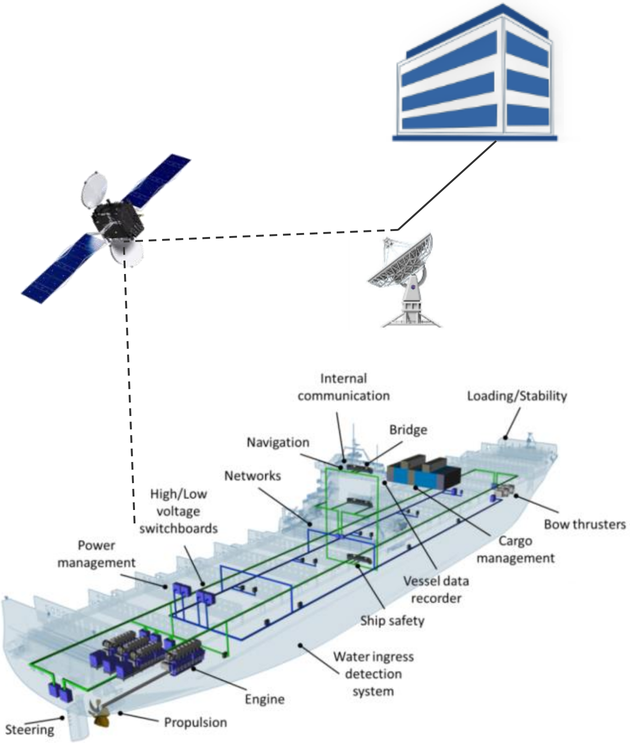
Safety in shipping today heavily depends on cyber systems

1950

60-70 YEARS

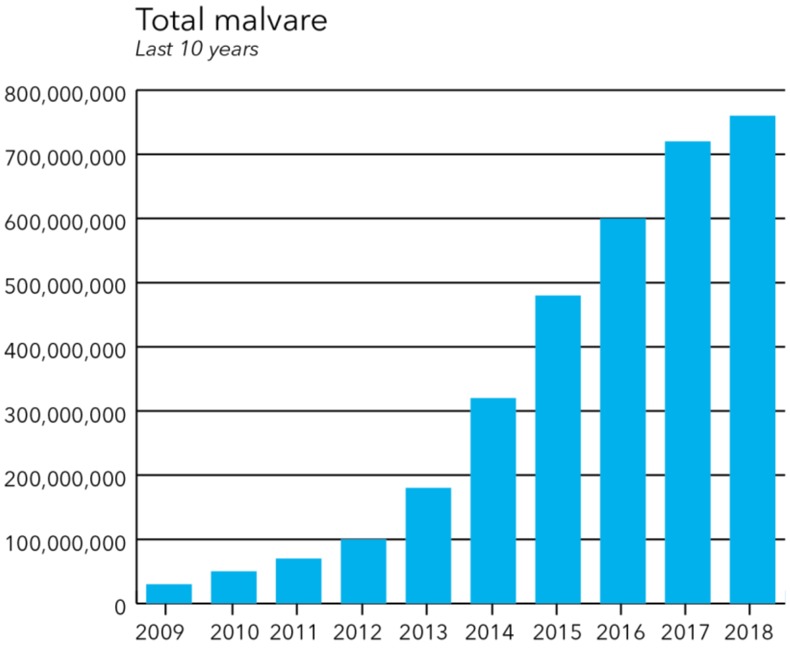
2018



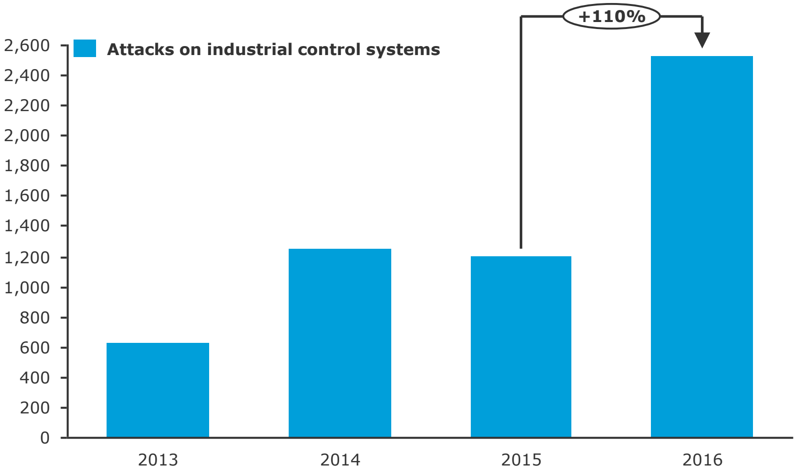


Cyber risks are present and migrating to the OT world

Information technology (IT)



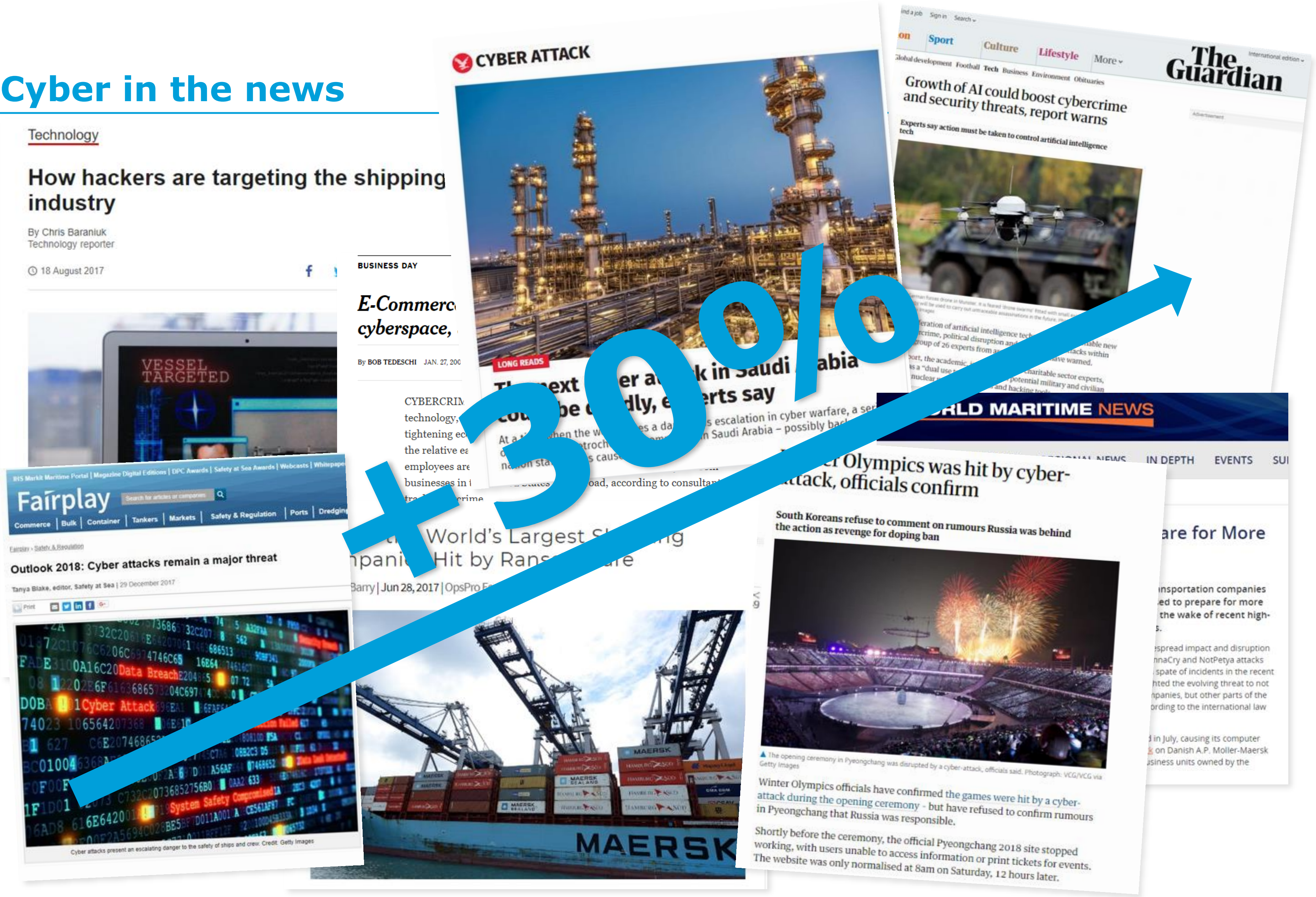
Operational technology (OT)



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)

Cyber in the news

+30%



Technology

How hackers are targeting the shipping industry

By Chris Baraniuk
Technology reporter

18 August 2017

VESSEL
TARGETED

BUSINESS DAY

E-Commerc
cyberspace,

By BOB TEDESCHI JAN. 27, 200

CYBERCRIM
technology,
tightening ec
the relative ea
employees are
businesses in t
tra crime

CYBER ATTACK

LONG READS

The next cyber attack in Saudi Arabia could be deadly, experts say

At a time when the w es a da s escalation in cyber warfare, a ser
d petroch n Saudi Arabia – possibly bac
nation sta s caus

States road, according to consultant

ind a job Sign in Search

on Sport Culture Lifestyle More

Global development Football Tech Business Environment Obituaries

The Guardian

International edition

Growth of AI could boost cybercrime and security threats, report warns

Experts say action must be taken to control artificial intelligence tech

Advertisement

eration of artificial intelligence tech able new
rcrime, political disruption and acks within
roup of 26 experts from a ave warned.
ort, the academic, charitable sector experts,
s a "dual use potential military and civilian
nuclear and hacking tools

RLD MARITIME NEWS

IN DEPTH EVENTS SU

are for More

nsportation companies
ed to prepare for more
the wake of recent high-
s.

espread impact and disruption
nnaCry and NotPetya attacks
spate of incidents in the recent
hted the evolving threat to not
npanies, but other parts of the
ording to the international law

in July, causing its computer
on Danish A.P. Moller-Maersk
usiness units owned by the

IHS Markit Maritime Portal | Magazine Digital Editions | DPC Awards | Safety at Sea Awards | Webcasts | Whitepape

Fairplay

Search for articles or companies

Commerce | Bulk | Container | Tankers | Markets | Safety & Regulation | Ports | Dredgin

Fairplay › Safety & Regulation

Outlook 2018: Cyber attacks remain a major threat

Tanya Blake, editor, Safety at Sea | 29 December 2017

Print

Cyber attacks present an escalating danger to the safety of ships and crew. Credit: Getty Images

World's Largest Shipping Companies Hit by Ransomware

Barry | Jun 28, 2017 | OpsPro

Winter Olympics was hit by cyber-attack, officials confirm

South Koreans refuse to comment on rumours Russia was behind the action as revenge for doping ban

The opening ceremony in Pyeongchang was disrupted by a cyber-attack, officials said. Photograph: VCG/VCG via Getty Images

Winter Olympics officials have confirmed the games were hit by a cyber-attack during the opening ceremony - but have refused to confirm rumours in Pyeongchang that Russia was responsible.

Shortly before the ceremony, the official Pyeongchang 2018 site stopped working, with users unable to access information or print tickets for events. The website was only normalised at 8am on Saturday, 12 hours later.

Incident trends and regulation development

2010

Drilling rig infected with malware

2011

Pirate Cyber Attack

2012

GPS jamming /spoofing

2013

Hacking of cargo tracking system

ISO 27001/27002

IEC 62443

2014

U.S. Port hacker attack

2016

Bulk carrier SWB shuts down – ransomeware

January BIMCO Cyber security guideline

IMO guidelines on cyber security onboard ships

July NIS directive

September DNVGL-RP-0496

2017

Major shipping company infected by ransomeware

July IMO guidelines on maritime cyber risk management

?

2018

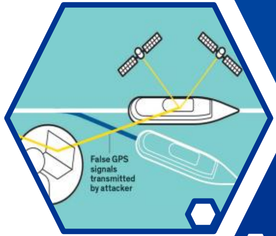
"Prepare for the unknown"

January DNV GL Cyber security Type Approval

May EU GDPR

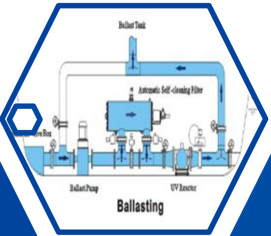
July DNV GL class notation

Reported incidents around the world is increasing



Loss of fuel control and ballast water valves due to ECDIS update

GPS jamming and spoofing



VSAT hacking using common login

AIS spoofing

PMS system shore and vessel attack

ECIDS ransomware and chart spoofing

Pirate attack supported by cyber attack

Loss of main switchboard due to ransomware

Malware allows full access to vessel systems

Hackers took "full control" of navigation systems for 10 h

Hacking of cargo tracking system for smuggling purposes

NotPetya cause Maersk upto USD 300m loss

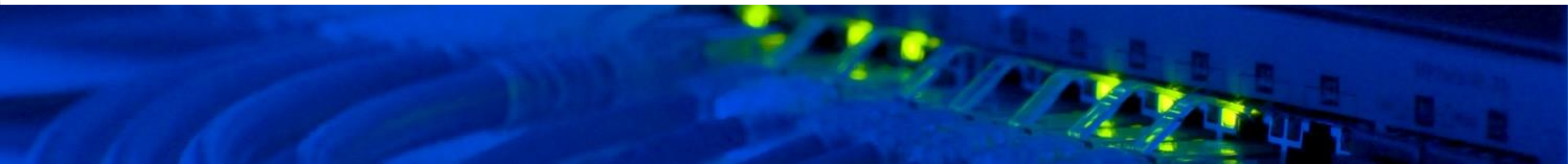
STRUCTURE

Status on cyber security in maritime shipping

RISK SCENARIOS (THREATS)

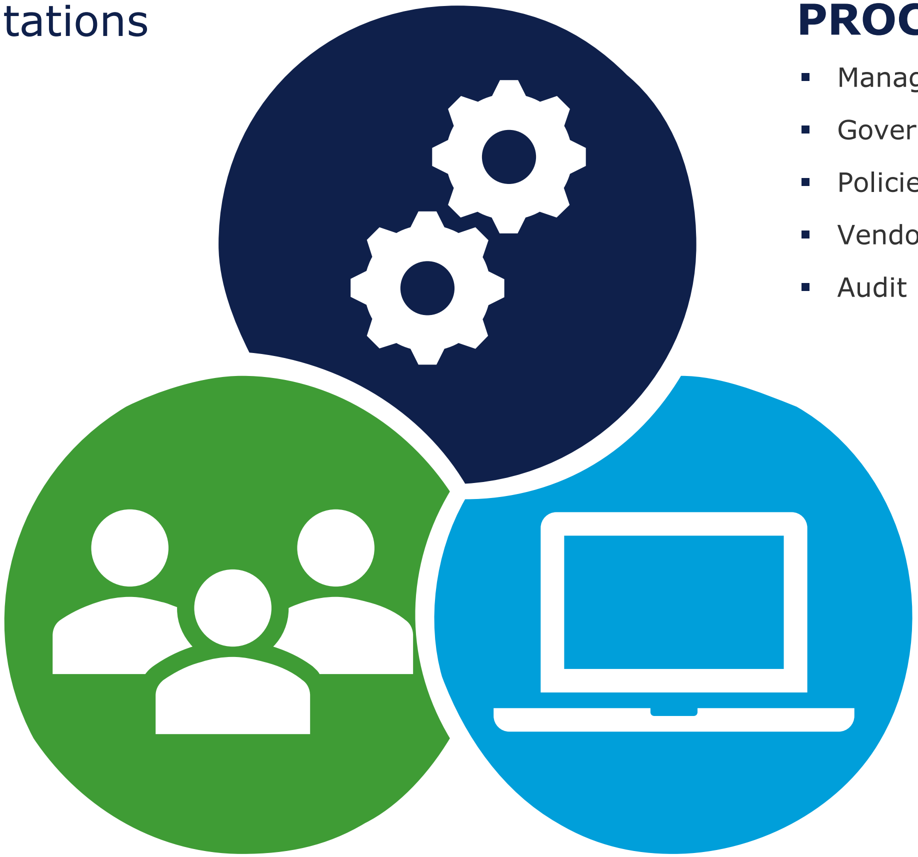
Best practices for you and your company

DNV GL and Gard and cyber security



It is not only about software and technology

The three pillars of cyber security implementations



PROCESS

- Management systems
- Governance frameworks
- Policies and procedures
- Vendor/Third party contract follow up
- Audit regimes

PEOPLE

- Training and awareness
- Professional skills and qualifications
- Written procedures
- Authorizations
- Physical security

TECHNOLOGY

- System design, design review
- Software configurations
- Inspection/verification
- Testing
  - Functional testing
  - Vulnerability scanning
  - Penetration test

Attackers come in many guises …

Why? Motivation

Disruption Espionage Financial

Threat agents

Outsiders

- Hacktivists
- Nation states
- Criminal organisations
- Terrorists
- Hackers and Amateurs

Insiders

- Criminal aims
- Disgruntled employees
- Unintentional

Some common threat scenarios for ship and crew

	Unintentional ("working accident", not following procedures)	**Bad intentions, planned**
Social engineering/phishing	✓	✓
Removable media/external hardware	✓	✓
Mixing isolated and open networks	✓	
Tampering with ECDIS, navigation systems	✓	✓
Ransomware (malware)	✓	✓
Denial of Service (DoS/DDoS)		✓
Data filtration/data theft		✓

Threat scenario

#1

SOCIAL ENGINEERING/PHISHING

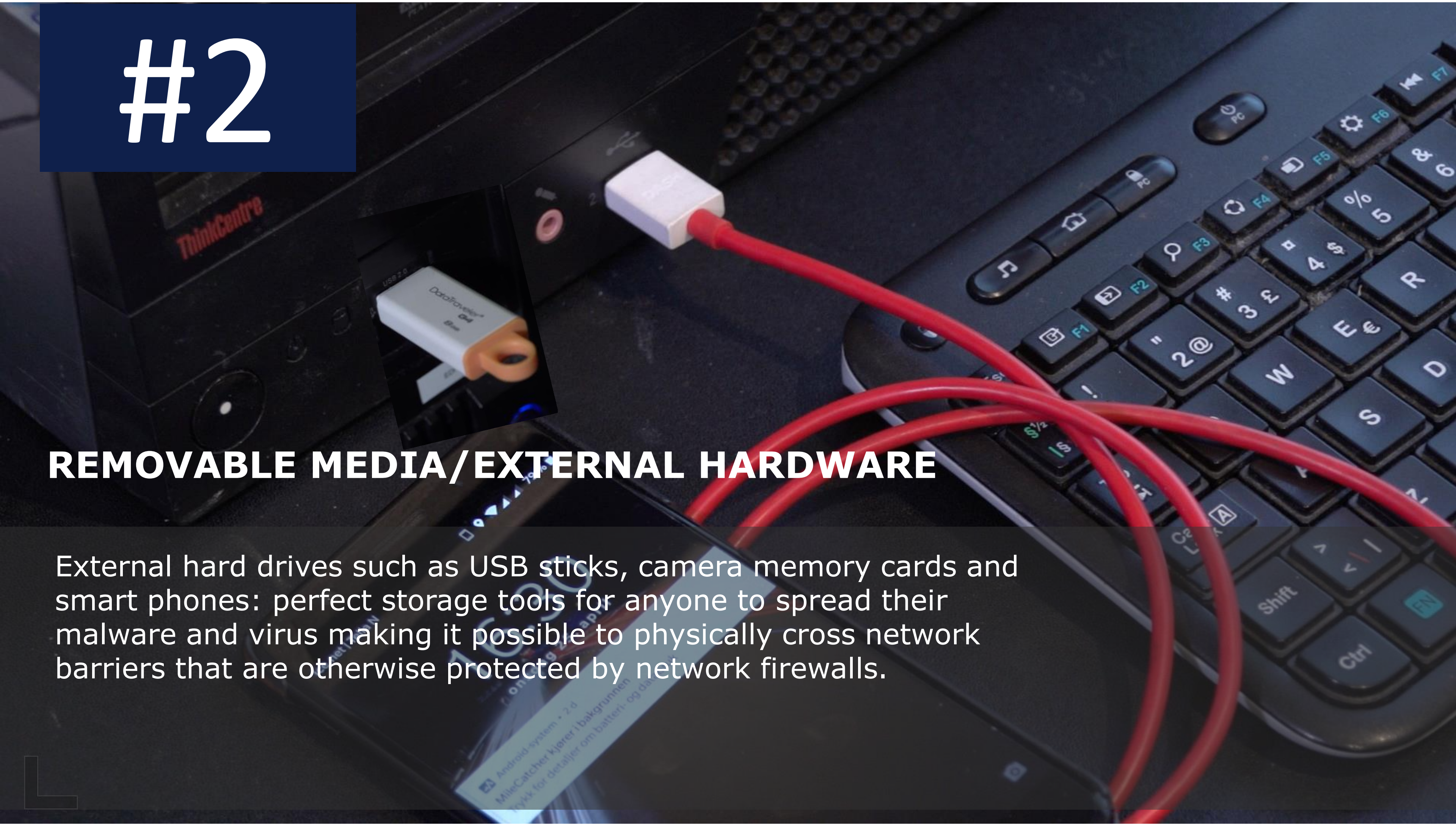
One of the most common forms of cyber crime is social engineering

This is the art of manipulating people by using methods like urgency, fear and curiosity

Reveals confidential information that can be used to gain unauthorized access to personal or company systems

Threat scenario

#2



REMOVABLE MEDIA/EXTERNAL HARDWARE

External hard drives such as USB sticks, camera memory cards and smart phones: perfect storage tools for anyone to spread their malware and virus making it possible to physically cross network barriers that are otherwise protected by network firewalls.

Threat scenario

#3

MIXING ISOLATED AND OPEN NETWORKS

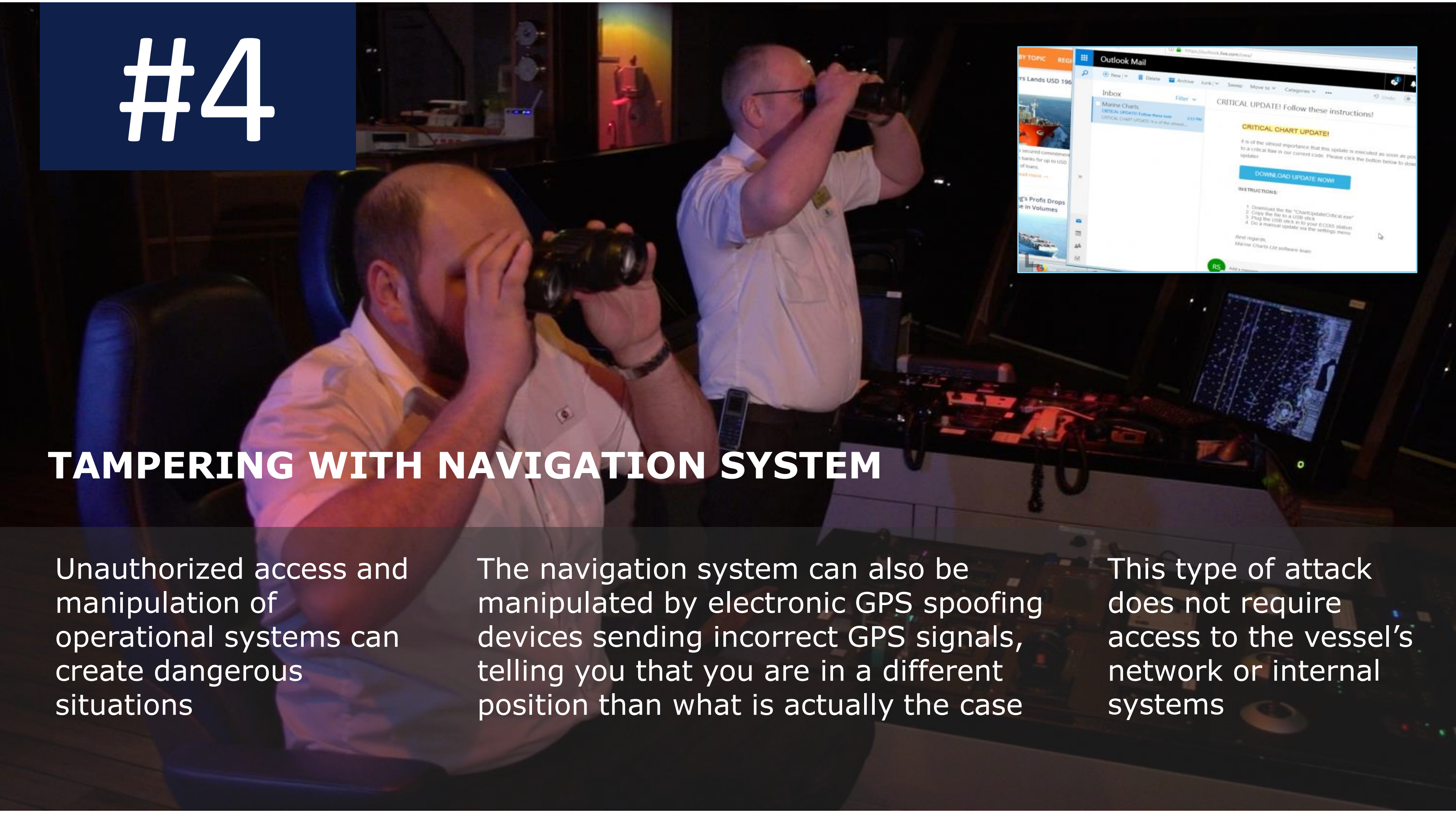
Connecting a personal wireless router or PC to the isolated network reserved for operational equipment is a major security risk.

Hackers can invade your systems by exploiting an open wireless network, or one with low level security.

They can literally sit outside your ship's physical location and access critical onboard systems through wireless networks.

Threat scenario

#4



Outlook Mail

https://outlook.live.com/owa/

Marine Charts
CRITICAL UPDATE! Follow these instr
CRITICAL CHART UPDATE! It is of the utmost...
2:13 PM

CRITICAL UPDATE! Follow these instructions!

CRITICAL CHART UPDATE!

It is of the utmost importance that this update is executed as soon as pos to a critical flaw in our current code. Please click the button below to dow updater.

INSTRUCTIONS:

1. Download the file "ChartUpdateCritical.exe"
2. Copy the file to a USB stick
3. Plug the USB stick in to your ECDIS station
4. Do a manual update via the settings menu

Best regards,
Marine Charts Ltd software team

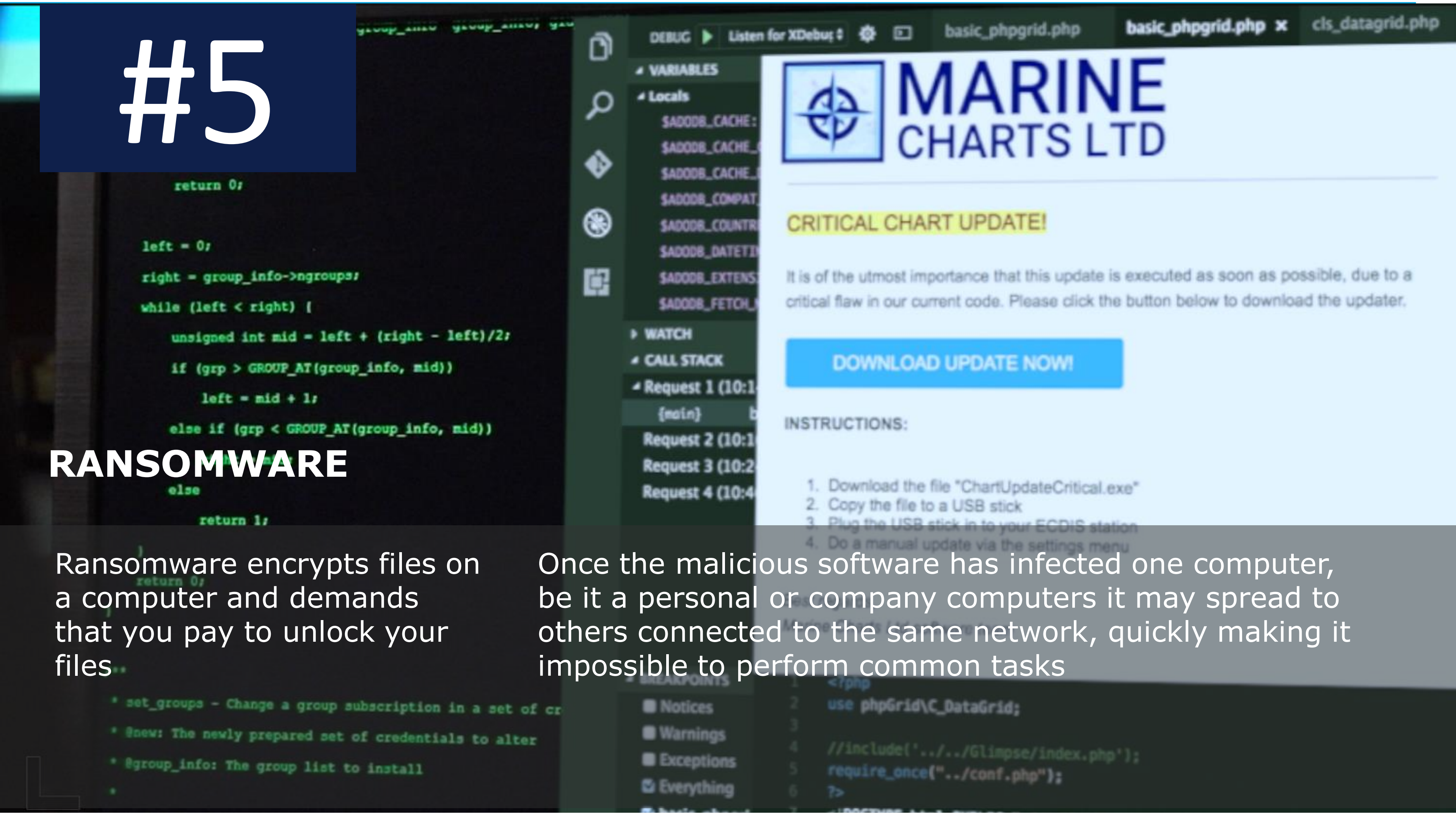
TAMPERING WITH NAVIGATION SYSTEM

Unauthorized access and manipulation of operational systems can create dangerous situations

The navigation system can also be manipulated by electronic GPS spoofing devices sending incorrect GPS signals, telling you that you are in a different position than what is actually the case

This type of attack does not require access to the vessel's network or internal systems

Threat scenario



```
return 0;

left = 0;
right = group_info->ngroups;
while (left < right) {
    unsigned int mid = left + (right - left)/2;
    if (grp > GROUP_AT(group_info, mid))
        left = mid + 1;
    else if (grp < GROUP_AT(group_info, mid))
    else
        return 1;
return 0;
 * set_groups - Change a group subscription in a set of cr
 * @new: The newly prepared set of credentials to alter
 * @group_info: The group list to install
 *
```

MARINE CHARTS LTD

CRITICAL CHART UPDATE!

It is of the utmost importance that this update is executed as soon as possible, due to a critical flaw in our current code. Please click the button below to download the updater.

DOWNLOAD UPDATE NOW!

INSTRUCTIONS:

1. Download the file "ChartUpdateCritical.exe"
2. Copy the file to a USB stick
3. Plug the USB stick in to your ECDIS station
4. Do a manual update via the settings menu

```
<?php
use phpGrid\C_DataGrid;
//include('../../Glimpse/index.php');
require_once("../conf.php");
?>
```

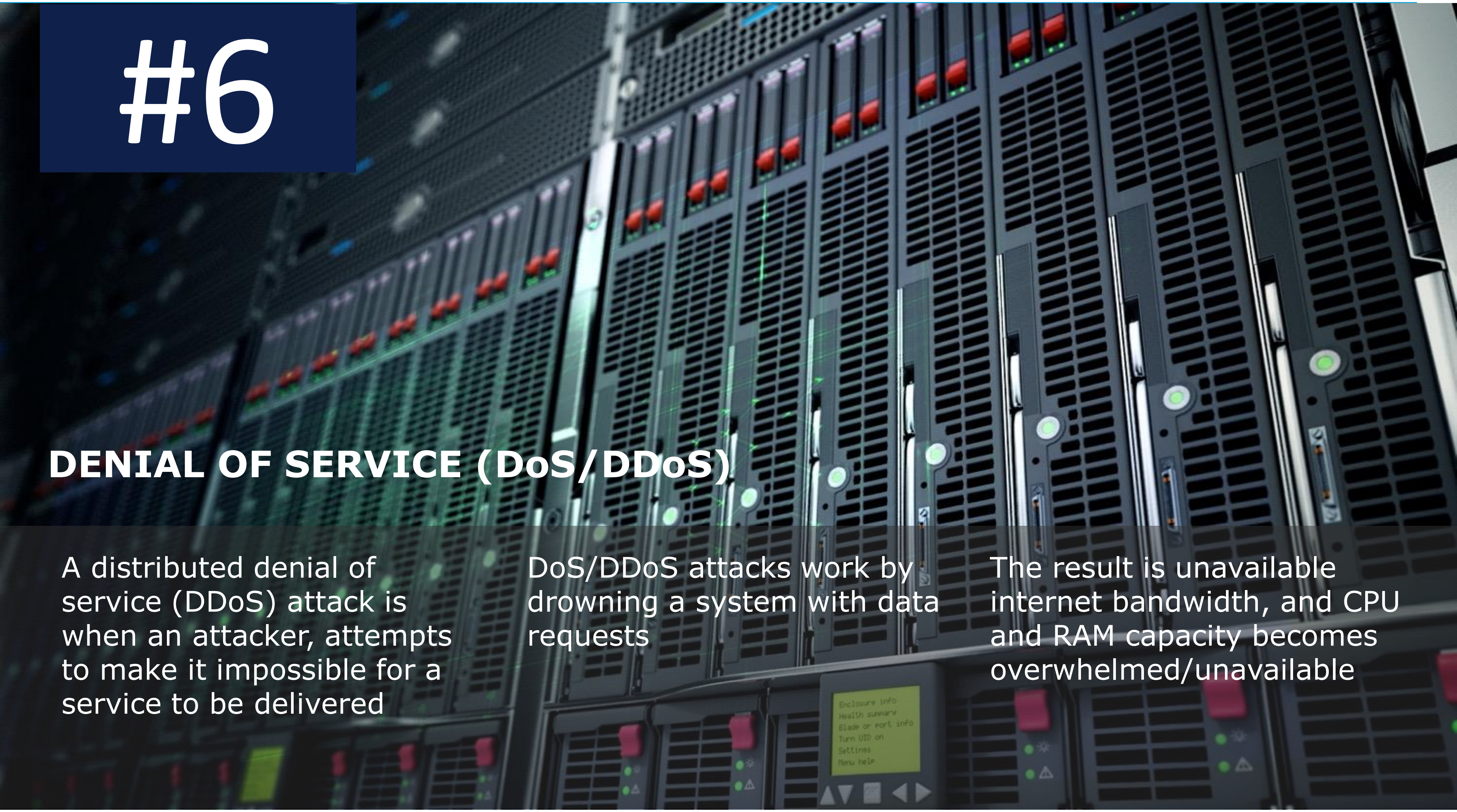
#5

RANSOMWARE

Ransomware encrypts files on a computer and demands that you pay to unlock your files

Once the malicious software has infected one computer, be it a personal or company computers it may spread to others connected to the same network, quickly making it impossible to perform common tasks

Threat scenario



#6

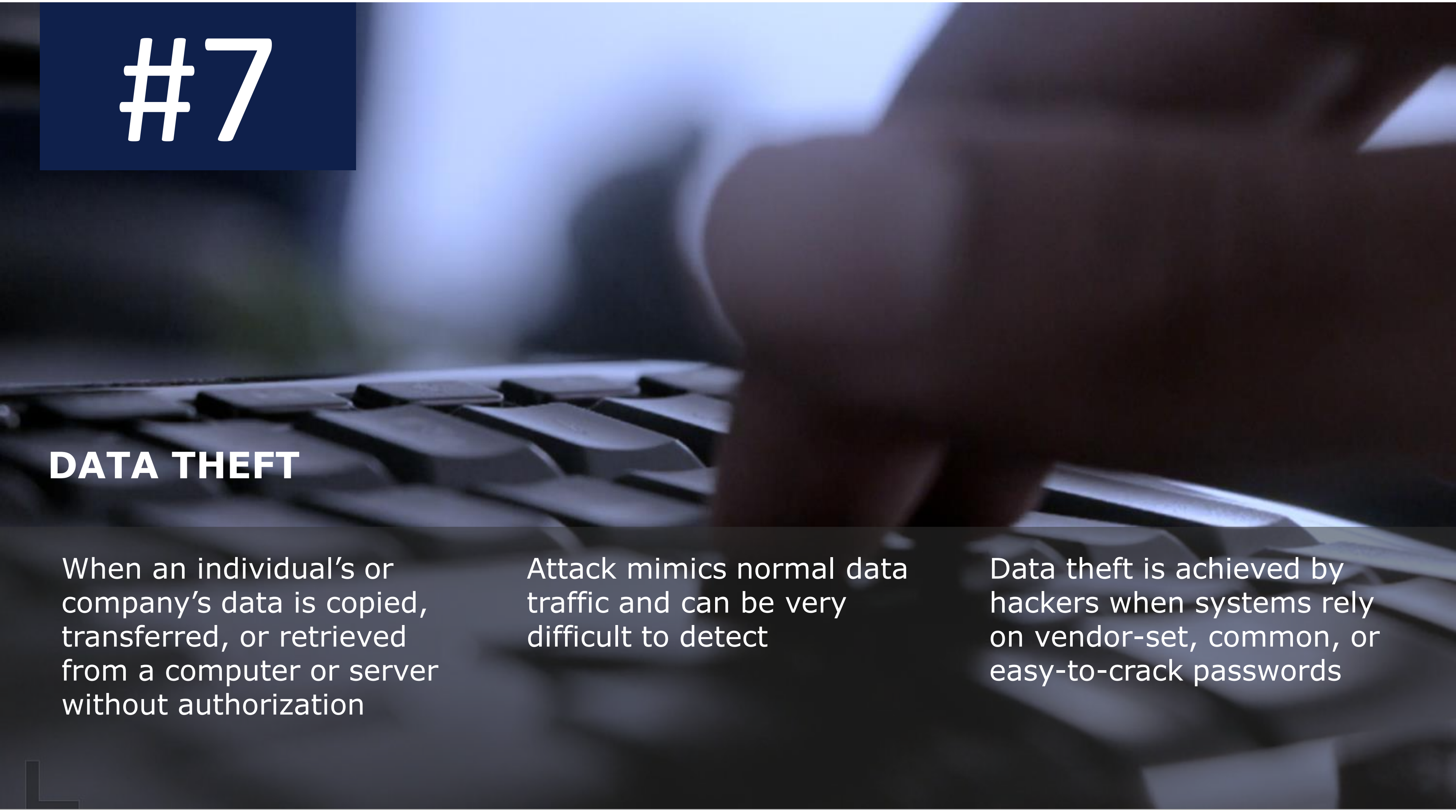
DENIAL OF SERVICE (DoS/DDoS)

A distributed denial of service (DDoS) attack is when an attacker, attempts to make it impossible for a service to be delivered

DoS/DDoS attacks work by drowning a system with data requests

The result is unavailable internet bandwidth, and CPU and RAM capacity becomes overwhelmed/unavailable

Threat scenario



#7

DATA THEFT

When an individual’s or company’s data is copied, transferred, or retrieved from a computer or server without authorization

Attack mimics normal data traffic and can be very difficult to detect

Data theft is achieved by hackers when systems rely on vendor-set, common, or easy-to-crack passwords

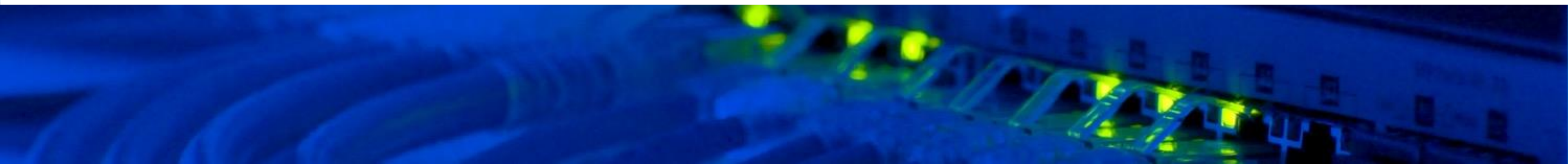
STRUCTURE

Status on cyber security in maritime shipping

Risk scenarios (threats)

BEST PRACTICES FOR YOU AND YOUR COMPANY

DNV GL and Gard and cyber security



Best practices how to avoid cyber mishaps onboard your ship/in your company

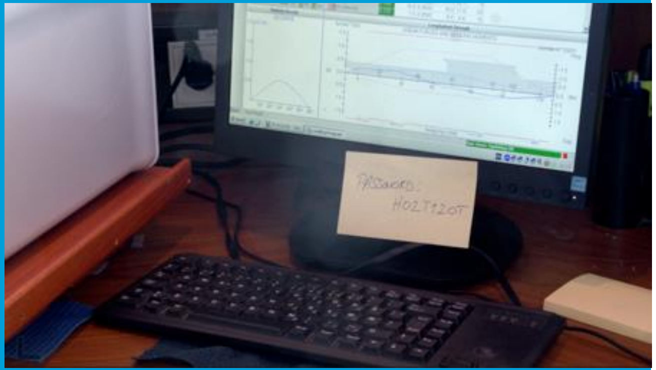
1. Think before you click!
2. Research the facts behind e-mails and their attachments!
3. Make sure external drives and USBs are clean!
4. Be aware when third parties enter your systems or data!
5. Protect your passwords!
6. Never connect personal items to the ship critical systems.
7. Never use external wi-fi for company emails or downloads unless protected by VPN!
8. Learn how to install and use two step authentication.
9. Learn how backup and restore is done onboard your ship.
10. Always report errors and mistakes.
11. Educate yourself on cyber risks and how it affects your ship, your colleagues and you personally!

1. **Think before you click!**
2. **Research the facts behind e-mails and their attachments!**
3. Make sure external drives and USBs are clean!
4. Be aware when third parties enter your systems or data!
5. Protect your passwords!
6. Never connect personal items to the ship critical systems.
7. Never use external wi-fi for company emails or downloads unless protected by VPN!
8. Learn how to install and use two step authentication.
9. Learn how backup and restore is done onboard your ship.
10. Always report errors and mistakes.
11. Educate yourself on cyber risks and how it affects your ship, your colleagues and you personally!

1. Think before you click!
2. Research the facts behind e-mails and their attachments!
3. **Make sure external drives and USBs are clean!**
4. Be aware when third parties enter your systems or data!
5. Protect your passwords!
6. Never connect personal items to the ship critical systems.
7. Never use external wi-fi for company emails or downloads unless protected by VPN!
8. Learn how to install and use two step authentication.
9. Learn how backup and restore is done onboard your ship.
10. Always report errors and mistakes.
11. Educate yourself on cyber risks and how it affects your ship, your colleagues and you personally!

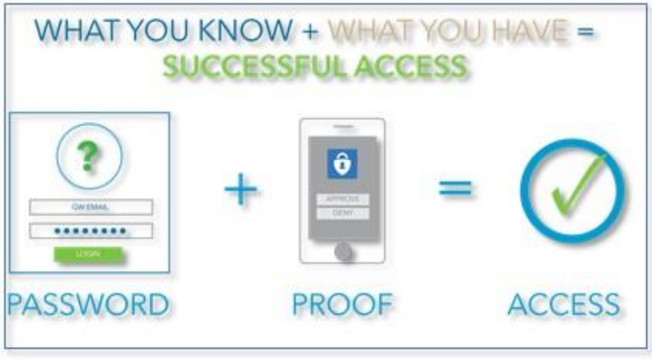
1. Think before you click!
2. Research the facts behind e-mails and their attachments!
3. Make sure external drives and USBs are clean!
4. **Be aware when third parties enter your systems or data!**
5. Protect your passwords!
6. Never connect personal items to the ship critical systems.
7. Never use external wi-fi for company emails or downloads unless protected by VPN!
8. Learn how to install and use two step authentication.
9. Learn how backup and restore is done onboard your ship.
10. Always report errors and mistakes.
11. Educate yourself on cyber risks and how it affects your ship, your colleagues and you personally!

1. Think before you click!
2. Research the facts behind e-mails and their attachments!
3. Make sure external drives and USBs are clean!
4. Be aware when third parties enter your systems or data!
5. **Protect your passwords!**
6. Never connect personal items to the ship critical systems.
7. Never use external wi-fi for company emails or downloads unless protected by VPN!
8. Learn how to install and use two step authentication.
9. Learn how backup and restore is done onboard your ship.
10. Always report errors and mistakes.
11. Educate yourself on cyber risks and how it affects your ship, your colleagues and you personally!



1. Think before you click!
2. Research the facts behind e-mails and their attachments!
3. Make sure external drives and USBs are clean!
4. Be aware when third parties enter your systems or data!
5. Protect your passwords!
6. **Never connect personal items to the ship critical systems.**
7. **Never use external wi-fi for company emails or downloads unless protected by VPN!**
8. Learn how to install and use two step authentication.
9. Learn how backup and restore is done onboard your ship.
10. Always report errors and mistakes.
11. Educate yourself on cyber risks and how it affects your ship, your colleagues and you personally!

1. Think before you click!
2. Research the facts behind e-mails and their attachments!
3. Make sure external drives and USBs are clean!
4. Be aware when third parties enter your systems or data!
5. Protect your passwords!
6. Never connect personal items to the ship critical systems.
7. Never use external wi-fi for company emails or downloads unless protected by VPN!
8. **Learn how to install and use two step authentication.**
9. Learn how backup and restore is done onboard your ship.
10. Always report errors and mistakes.
11. Educate yourself on cyber risks and how it affects your ship, your colleagues and you personally!

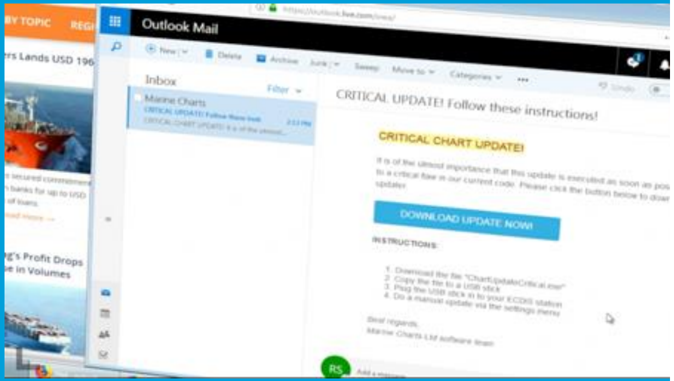


1. Think before you click!
2. Research the facts behind e-mails and their attachments!
3. Make sure external drives and USBs are clean!
4. Be aware when third parties enter your systems or data!
5. Protect your passwords!
6. Never connect personal items to the ship critical systems.
7. Never use external wi-fi for company emails or downloads unless protected by VPN!
8. Learn how to install and use two step authentication.
9. **Learn how backup and restore is done onboard your ship.**
10. Always report errors and mistakes.
11. Educate yourself on cyber risks and how it affects your ship, your colleagues and you personally!

1. Think before you click!
2. Research the facts behind e-mails and their attachments!
3. Make sure external drives and USBs are clean!
4. Be aware when third parties enter your systems or data!
5. Protect your passwords!
6. Never connect personal items to the ship critical systems.
7. Never use external wi-fi for company emails or downloads unless protected by VPN!
8. Learn how to install and use two step authentication.
9. Learn how backup and restore is done onboard your ship.

10. Always report errors and mistakes.

11. Educate yourself on cyber risks and how it affects your ship, your colleagues and you personally!



CRITICAL UPDATE! Follow these instructions!

CRITICAL CHART UPDATE!

It is of the utmost importance that this update is executed as soon as pos
to a critical flaw in our current code. Please click the button below to dow
update.

DOWNLOAD UPDATE NOW!

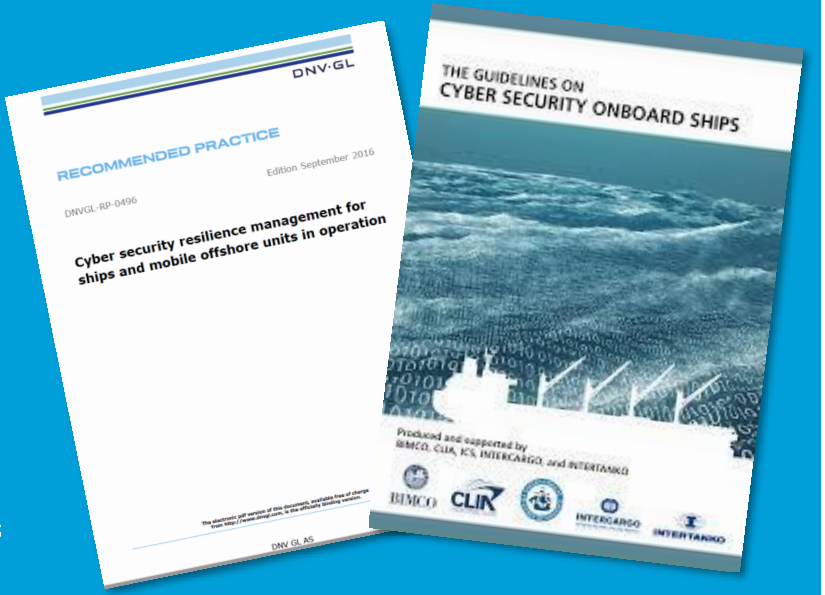
INSTRUCTIONS:

1. Download the file "ChartUpdateCritical.exe"
2. Copy the file to a USB stick
3. Plug the USB stick in to your ECDIS station
4. Do a manual update via the settings menu

Best regards,
Marine Charts Ltd software team

1. Think before you click!
2. Research the facts behind e-mails and their attachments!
3. Make sure external drives and USBs are clean!
4. Be aware when third parties enter your systems or data!
5. Protect your passwords!
6. Never connect personal items to the ship critical systems.
7. Never use external wi-fi for company emails or downloads unless protected by VPN!
8. Learn how to install and use two step authentication.
9. Learn how backup and restore is done onboard your ship.
10. Always report errors and mistakes.

11. Educate yourself on cyber risks and how it affects your ship, your colleagues and you personally!



DNV·GL

RECOMMENDED PRACTICE

DNVGL-RP-0496

Edition September 2016

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

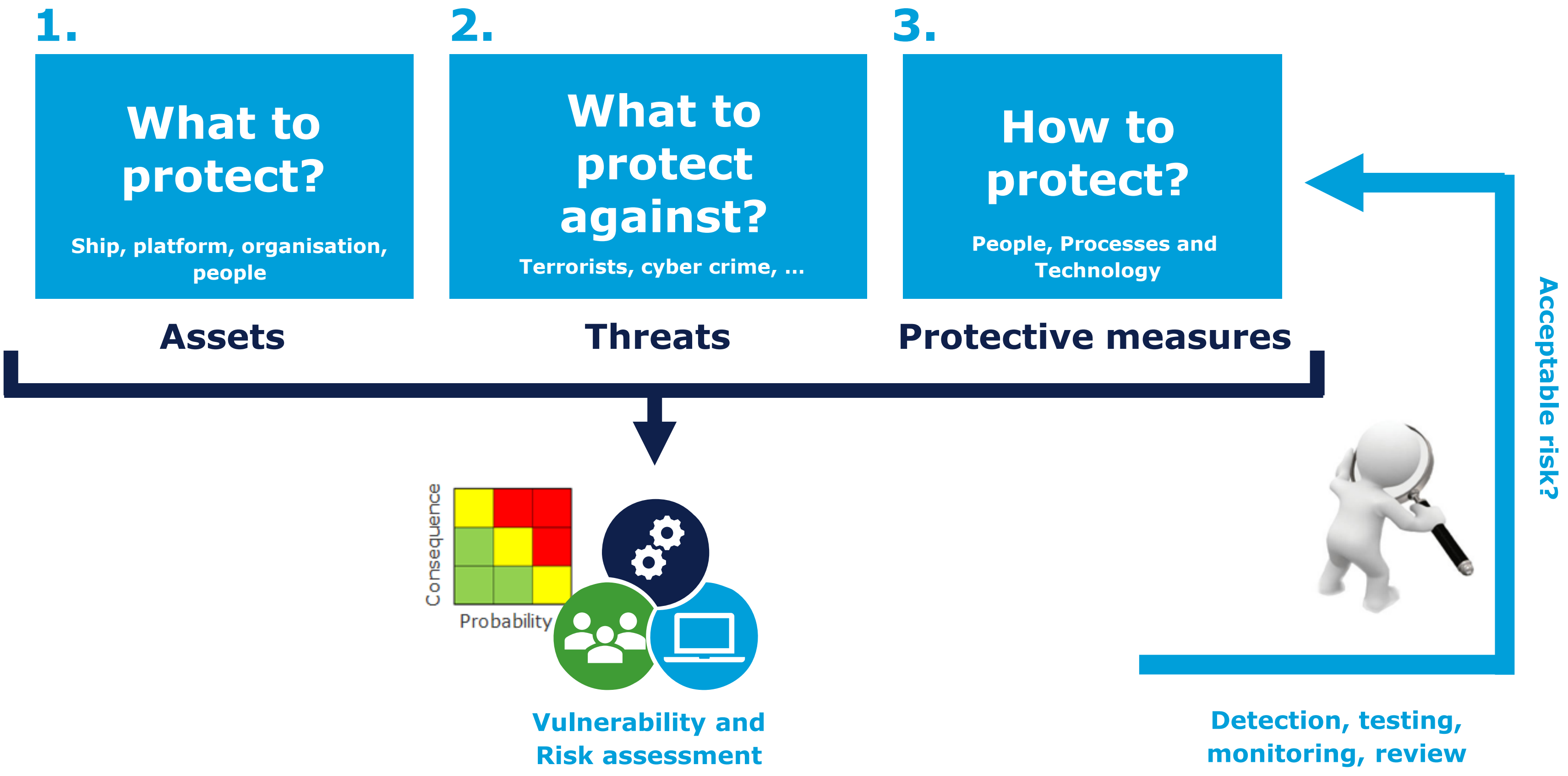
The electronic pdf version of this document, available free of charge from http://www.dnvgl.com, is the officially binding version.

DNV GL AS

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS

Produced and supported by BIMCO, CLIA, ICS, INTERCARGO and INTERTANKO

Cyber Security in a nutshell – a continuous approach!



1\.

What to protect?

Ship, platform, organisation, people

Assets

2\.

What to protect against?

Terrorists, cyber crime, …

Threats

3\.

How to protect?

People, Processes and Technology

Protective measures

Vulnerability and Risk assessment

Detection, testing, monitoring, review

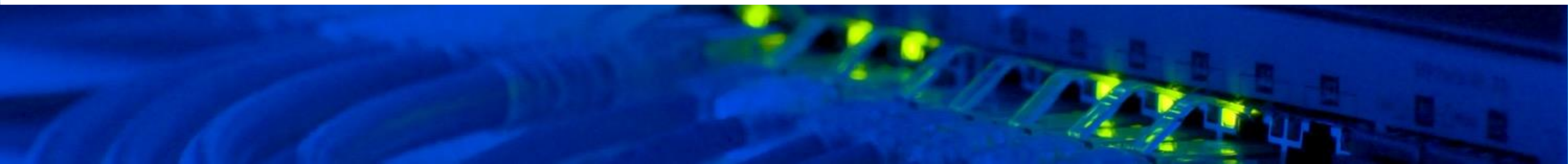
STRUCTURE

Status on cyber security in maritime shipping

Risk scenarios (threats)

Best practices for you and your company

DNV GL AND GARD AND CYBER SECURITY



DNV GL for managing risk, improving safety and performance

We support business-critical activities across industries, including maritime, oil and gas, energy and healthcare

Industry software solutions

Data management and analytics

Consulting and advisory services

Industry data platform

Cyber security

DNV GL CyberSecurity services

RISK ASSESSMENT

- System analysis and document review
- Inspection, interviews, workshops
- Self assessment

CYBERSECURITY TESTING

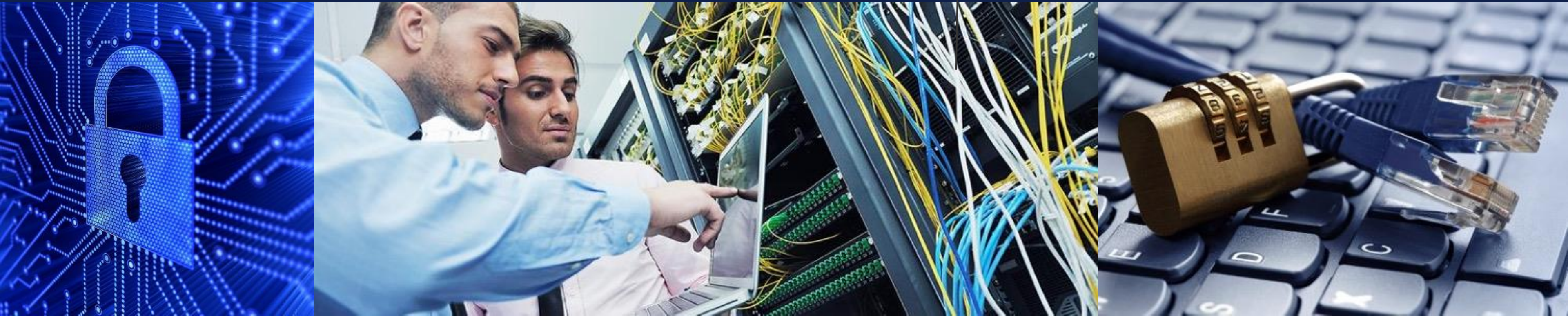
- Onboard audit
- Vulnerability analysis and Penetration testing
- Network health testing

CYBERSECURITY TRAINING

- Cybersecurity training and awareness
- Workshops and e-learning
- Phishing campaigns

CYBERSECURITY COMPLIANCE

- Type approval (TA): Applies to any component connected to a network
- Class notation
- GDPR, other standards/requirements



Gard Loss prevention awareness

- The easiest and most common way for cyber criminals to strike, is through **negligent or poorly trained individuals**

- Common perception among crew, doubting the importance of cyber security

- Cyber risk is related to operational procedures and **crew training**, not just the IT hardware and OT systems

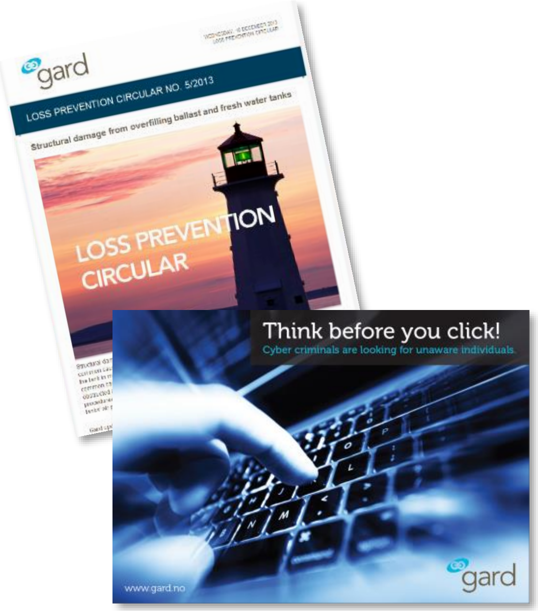
Warning
Is your download free of malware?
Most data breaches are caused by authorised users.
Yes
No
Cancel
www.gard.no
gard

Gard Loss prevention products

Experience transfer and knowledge sharing based on real cases

Cyber security awareness in the maritime industry

There is no single solution to managing cyber risks. It is a collaboration involving people, processes and IT systems. Establishing awareness in all levels of an organisation is the important first step when implementing cyber security management.


gard
LOSS PREVENTION CIRCULAR NO. 5/2013
Structural damage from overfilling ballast and fresh water tanks
LOSS PREVENTION CIRCULAR
Think before you click!
Cyber criminals are looking for unaware individuals.
www.gard.no
gard

gard
CASE STUDY NO. 35: SAMPLING
Case study for onboard safety meeting
CASE STUDY
Protect your weak links.
Cyber criminals are looking for weak links in your system.
VDR
Integrated Bridge Systems
Positioning Systems
Engine Telegraph / Steering Telemotors
ECDIS
BNWAS
GMDSS Console And Internal Communication
Anchor and Mooring Winch Control System
Bow Thruster Control System
Water Ingress Detection System
Steering Motors / Rudder Angle Indicator
Cargo Control And Monitoring Systems
Engine Control And Monitoring Systems
www.gard.no
gard

Alerts and posters for
AWARENESS

Circulars, Insights, videos for
LEARNING

Case studies for
DISCUSSION

www.dnvgl.com

Legal notice: *This presentation has been made in collaboration with Gard. The presentation is not meant to constitute an operational tool. It is intended purely as awareness material and guidance to be used at user’s own risk, and no warranties or representations are given nor are any duty of care or responsibility accepted by Gard or DNV-GL for any consequences whatsoever resulting directly or indirectly from compliance with or reliance on any guidance or advice contained in the presentation even if caused by a failure to exercise reasonable care on the part of any of the aforementioned parties*

SAFER, SMARTER, GREENER