MARIKO

WATERWAY IT SOLUTIONS

Waterway IT Solutions

The Sea is Always Changing. So Are We.

Florian zum Felde
IT Security
November 2021

BREAKING NEWS

Cyber incidents are flooding the news

DW

Kaseya cyberattack: Hackers want $70 million for decryption

Which companies were hit in this latest ransomware attack? The Miami-based firm Kaseya said a broad array of small businesses — including in...

05.07.2021

https://lloydslist.maritimeintelligence.informa.com/LL1138256/Shipping-needs-to-be-vigilant-over-cyber-risks

TheDigitalHacker

Ransomware attack on MediaMarkt disrupted some their ...

MediaMarkt was hit by a ransomware attack late Sunday night into Monday morning, encrypting servers and workstations and forcing the...

vor 2 Stunden

https://www.dw.com/en/kaseya-cyberattack-hackers-want-70-million-for-decryption/a-58158481

Splash 247

CMA CGM hit by another cyber attack - Splash247

CMA CGM has been hit by another cyber attack, just under one year since its last big breach. The French containerline told customers today...

vor 1 Monat

https://thedigitalhacker.com/ransomware-attack-on-mediamarkt-disrupted-some-their-services/

The Maritime Executive

Cyberattack Hits Multiple Greek Shipping Firms

"A cyber-attack incident cannot spoil the image we have created for 36 years," CEO Dimitris Theodosiou told Mononews. A cybersecurity expert...

vor 5 Tagen

https://www.maritime-executive.com/article/cyberattack-hits-multiple-greek-shipping-firms

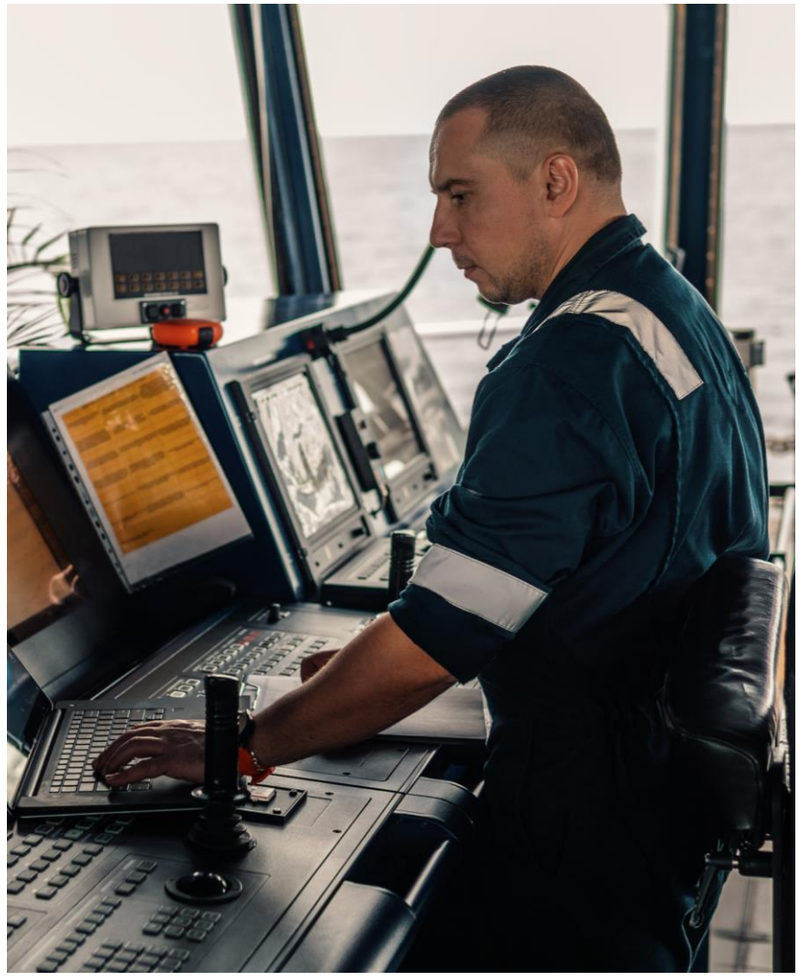
Cybercrime in shipping is no longer a ghost story, but a fact we have to deal with.

Seafarer Training for CyberSecurity

Maritime Cyber Security

"Amateurs hack systems, professionals hack people."

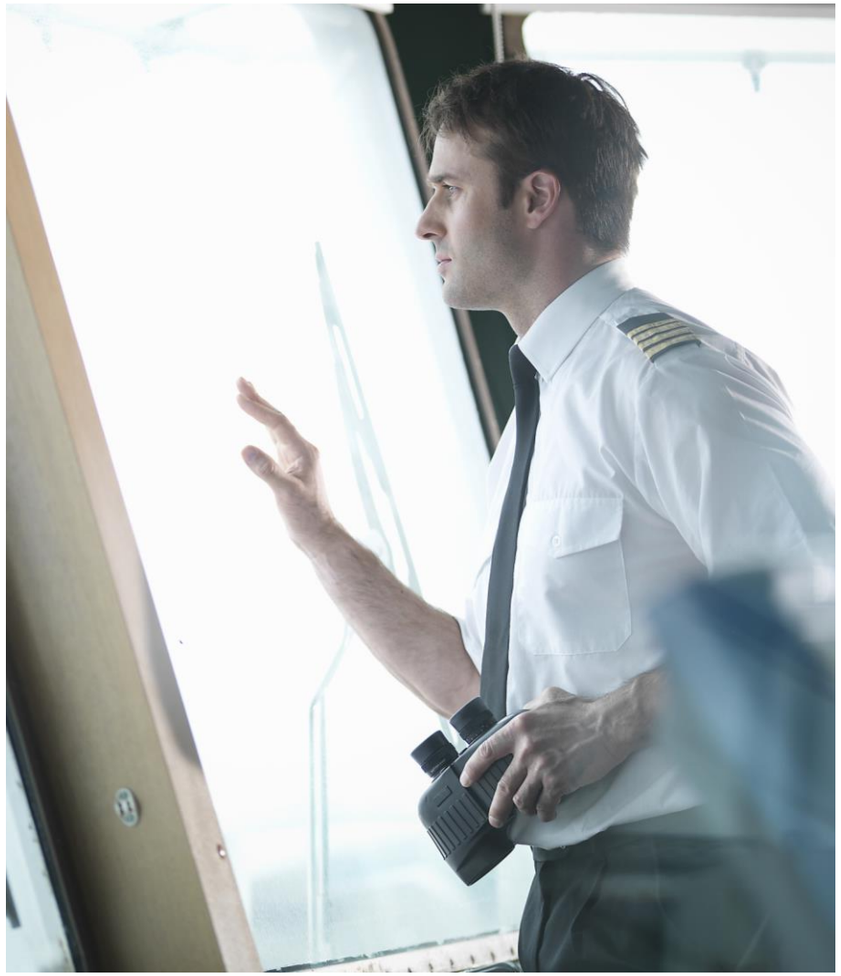
(Bruce Schneier)



What challenges does the crew face?

- Lack of IT knowledge
- No time to deal with IT issues
- Constantly changing and evolving IT systems
- Insufficient training for newly introduced systems
- IT issues where the crew is on its own
- Missing familiarization with IT procedures
- Cyber threat awareness and understanding

Crew are often not adequately trained or even able to deal with IT requirements on board.



Hazards for ship operation and business?

Risk to safety, security and economic interests

- Manipulation or failure of navigation systems
- Unauthorized access to monitoring and control systems
- Breakdown of the onboard communication systems
- Unintentional disclosure of security-related and sensitive information
- Financial loss due to off-hire and repair
- Damage to reputation

Failure or manipulation of on-board IT systems poses a risk to safety, security and economic interests.

Real Phishing Attack

E-Mail Sample

Harbour Master Req Dec Crewmember.docx
13 KB

SHIP NIL LIST.doc
34 KB

From: Harbour_Office (Capt) <captain@harbouroffice.org>
Sent: Saturday, 12. December 2020 14:23
To: Vessel Name <vesselname@shippingcompany.com>
Subject: Re: Vessel Name - PSC- Las Palmas agent details

DEAR CAPTAIN
GOOD DAY,

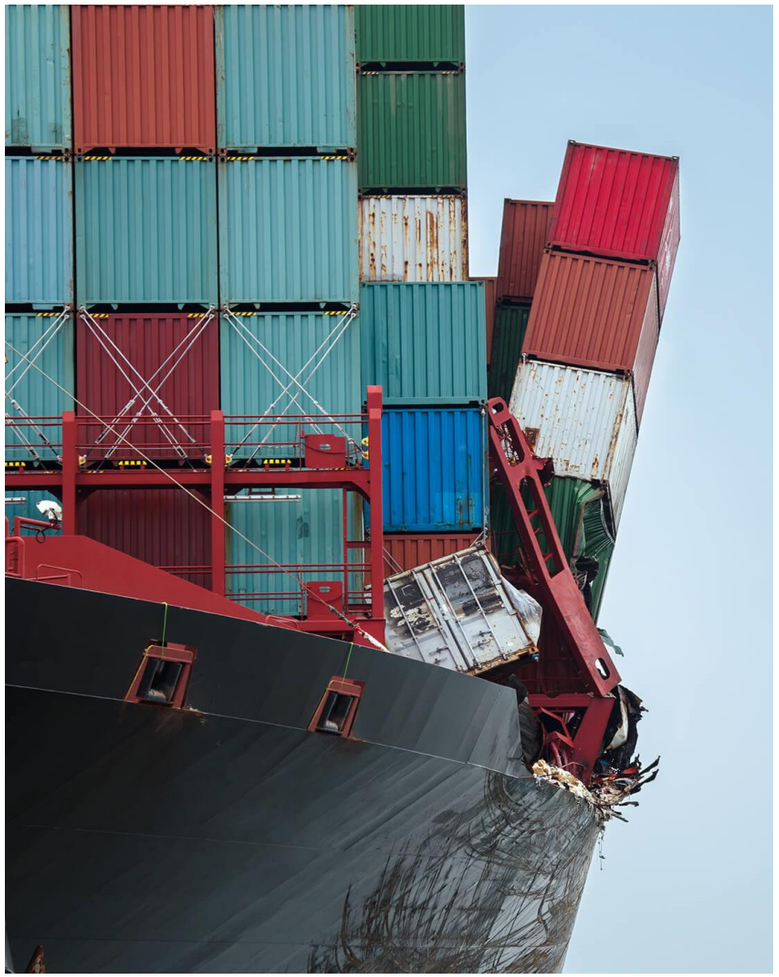
PLEASE RETURN THE COMPLETED FORM ATTACHED "HARBOUR MASTER DECLARATION"
AND REVERT US WITH "CREW LIST/PORT OF CALL LIST" VIA EMAIL.

N.B.
1 - ALL DOCUMENTS SHOULD BE SENT IN (PDF) FILE
2 - ALL DOCUMENTS SHOULD BE SENT WITH MASTER APPROVAL (SIGN+STAMP)

PLEASE REFER AS SOON AS POSSIBLE TO RECORD DATA IN OUR SYSTEM OF PORT.

PLEASE REPLY VIA : CAPTAIN[AT]HARBOUROFFICE.ORG

REGARDS
CAPT. ANONYMOUS | PSC
PORT STATE CONTROL
DIRECT EMAIL: CAPTAIN[AT]HARBOUROFFICE.ORG



Phishing Attack Security Check

Sample E-Mail

FROM: <Sarah Martin|Finance> “administration@fakecompanydomain.com”
SUBJECT: VESSEL NAME - INVOICE 00174245AV SHIPPING COMPANY NAME

Dt : 06/16/2021

To : [Shipping Company Name]
Attn. REAL DEPARTMENT NAME
Acc . M/V VESSEL NAME - Pending Invoice

Dear Sirs
Good Day,

VESSEL NAME - Outstanding Invoice no 00174245AV

Please review the reason for delaying the payment of your ship's invoice no: 00174245AV until today.

Link to the invoice for your reference: Invoice 00174245AV

We look forward to hearing from you.

Yours sincerely,
Sarah Martin

FAKE COMPANY
SERVING THE SHIPPING INDUSTRY

Mrs.Sarah Garcia Martin
Financial Assistant.

Simulated Phishing Attack

Sample Report

Dispatch rate (292 / 292)

100%

Error rate: 0% (0 / 292)

Open rate (269 / 292)

92.1%

Click rate (90 / 292)

30.8%

clicked

not clicked

Interaction rate (44 / 90)

48.9%

Reply rate (31 / 292)

10.6%

Every click or response poses a major security risk.
With recurring security campaigns, you train your crew to act wisely in the right moment.

Crew members require support

Training needs

- Dealing with threats from e-mail attacks
- Internet Usage & Social Media
- Handling of private devices
- Protection of user information & passwords
- Authorization of third-party access (on board or remote)
- Procedures for IT maintenance
- Understanding the threats to ship operations
- Reasonable familiarization with all relevant IMO 2021 IT procedures

Crew are often not adequately trained or even able to deal with IT requirements on board.

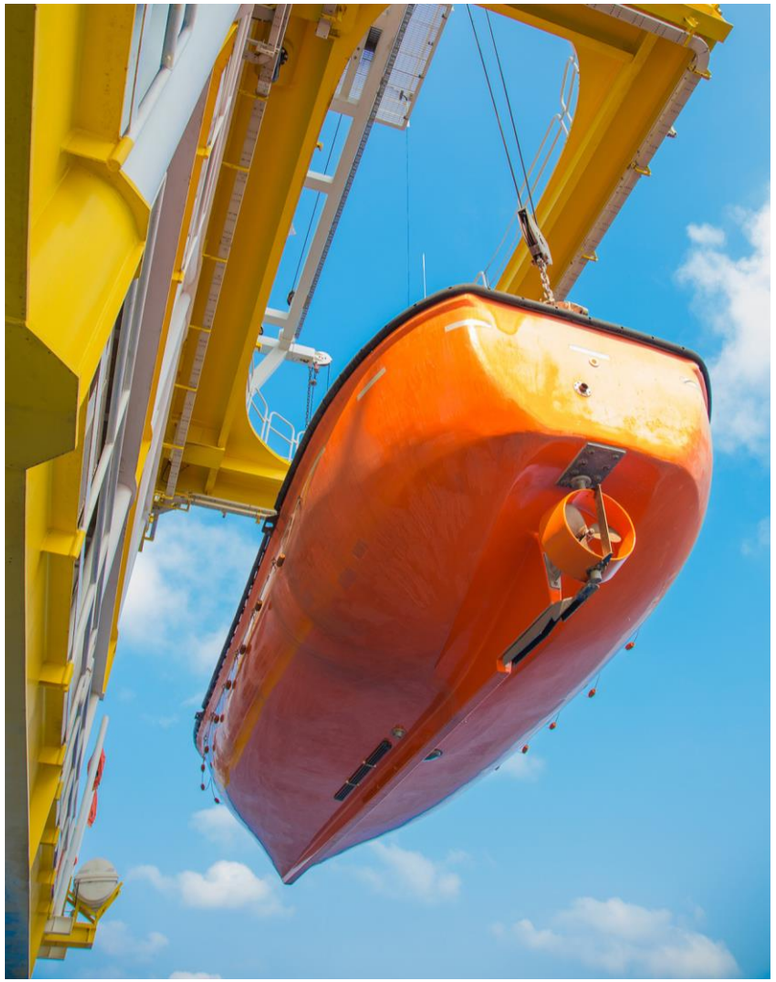
What do I have to consider?

Training measures

- Plan training sessions close to practice, relevant and attractive
- Organize recurring security awareness campaigns
- Check on a regular basis whether the training activities were successful
- Reasonable familiarization with all relevant IMO 2021 matters
- Involve maritime IT experts if no in-house know-how is available

"The first step towards a change in behavior is awareness. Seafarers and offshore crew need to understand the threats before they can mitigate the risk".

(Giles Noakes)



Seafarer Training for CyberSecurity

Maritime Cyber Security

“Technical security systems are crucial, but don't forget the human firewall”.

(Waterway IT)

Thank You!

The Sea is Always Changing. So Are We.

Waterway IT Solutions GmbH & Co. KG

Palmaille 67
D-22767 Hamburg
Germany

+49 (40) 28428- 5800
info@waterway-it.com
www.waterway-it.com

360° Vessel IT

Communication & Cyber Security

Vessel IT Consulting