CYBER SECURITY AWARENESS
in the maritime industry

Jarle Fosen, Senior Loss Prevention Executive
January 2019
Why do cyber incidents happen?
MODERN CRIMINALS USE KEYBOARDS, NOT GUNS

OBJECTIVES

Cyber attack

- Destruction of Data
- Publication of sensitive data
- Espionage
- Media Attention
- Selling stolen data
- Financial Gains
- Gaining knowledge
- Ransoming stolen data
- Ransoming system operability
- Arranging fraudulent cargo transportation
INTRODUCTION

CYBER SECURITY AWARENESS
in the Maritime Industry
AN INCREASINGLY DIGITISED SHIP
IT & OT SYSTEMS ONBOARD
BUSINESS BENEFITS FROM CONNECTING
OPERATIONAL TECHNOLOGY (OT)

- Autonomy: Efficiency in operations
- Knowledge: Prediction & diagnostics
- Direct Running Cost: Optimal maintenance
- Availability: Remote support
... so what may the consequences be from a cyber incident?
CONSEQUENCES OF A CYBER ATTACK

• Business interruption – including disruption to the port’s activities
• Physical loss of or damage to ship
• Loss of cargo
• Pollution
• Physical injury to crew
MAERSK CYBER INCIDENT
...EVEN THE BEST CAN BE HIT BY THE WORST

June 2017 – worldwide malware meltdown

Modified Petya ransomware that hit Ukraine hard on June 27, 2017, also disrupted computers at Russia's largest oil company, European banks, and multinational corporations.

Petya (or NotPetya or Nyetya)
BW GROUP CYBER INCIDENT
...EVEN THE BEST CAN BE HIT BY THE WORST

BW Group which commands USD 2.0 bn LNG fleet & USD 2.1 bn LPG fleet came under attack in July 2017

Internet and intranet systems were closed down temporarily
CYBER TREND
INCIDENTS AND REGULATION

2010
Drilling rig infected with malware

2011
Pirate Cyber Attack

2012
GPS jamming /spoofing

2013
Hacking of cargo tracking system

2014
U.S. Port hacker attack

2016
Bulk carrier SWB shuts down – ransomware

2017
Major shipping company infected by ransomware

2018
“Prepare for the unknown”

January
ISO 27001/27002
IEC 62443

BIMCO Cyber security guideline

February
ABS Guidance note
LR Guidance note

September
DNV-GL guideline

July
IMO guidelines
Maritime cyber risk management

May
EU GDPR

July
DNV-GL class notation
Information technology
- IT Networks
- Emails
- Administration, access, crew lists, …
- PMS
- Stores requisitions
- Electronic manuals
- Electronic certificates
- Permits to work
- Charter party, notice of readiness, bill of lading..

Operation technology
- PLC (Programmable Logic Controllers)
- SCADA (supervisory control and data acquisition)
- On-board measurement and control
- ECDIS
- GPS
- Remote support for engines
- Loggers
- Engine & Cargo control
- Dynamic positioning, …
Information technology (IT)

Operational technology (OT)

Source: AV-TEST Institute, Germany & IBM Managed Security Services)
Protocols

The following protocols are some of the languages that the industrial control systems use to communicate across the internet. Many of them were developed before the internet became widely used, which is why Internet-accessible ICS devices don’t always require authentication – it’s just part of the protocol.

**Siemens**

Modbus is a popular protocol for industrial control systems (ICS). It provides easy, raw access to the control system without requiring any authentication.

[Explore Modbus](https://www.shodan.io/explore/category/industrial-control-systems)

**DNP3** (Distributed Network Protocol) is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies.

[Explore DNP3](https://www.shodan.io/explore/category/industrial-control-systems)

**BACnet**

BACnet is a communications protocol for building automation and control networks. It was designed to allow communication of building automation and control systems for applications such as heating, air-conditioning, lighting, and fire detection systems.

[Explore BACnet](https://www.shodan.io/explore/category/industrial-control-systems)

**EtherCAT**

EtherCAT/IP was introduced in 2001 and is an industrial Ethernet network solution available for manufacturing automation.

[Explore EtherCAT/IP](https://www.shodan.io/explore/category/industrial-control-systems)

**HART**

HART (Highway Addressable Remote Transducer Protocol) is an early implementation of Fieldbus, a digital industrial automation protocol. Its most notable advantage is that it can communicate over legacy wiring.

[Explore HART](https://www.shodan.io/explore/category/industrial-control-systems)

**GE-SRTP**

Service Request Transport Protocol (GE-SRTP) protocol is developed by GE Intelligent Platforms (earlier GE Fanuc) for transfer of data from PLCs.

[Explore GE-SRTP](https://www.shodan.io/explore/category/industrial-control-systems)

**PCoIP**

PCoIP is a protocol and program by Phoenix Contact used by a wide range of industries.

[Explore PCoIP](https://www.shodan.io/explore/category/industrial-control-systems)

**MELSEC-Q** Series use a proprietary network protocol for communication. The devices are used by equipment and manufacturing facilities to provide high-speed, large volume data processing and machine control.

[Explore MELSEC-Q](https://www.shodan.io/explore/category/industrial-control-systems)

**OMRON**

FINS, Factory Interface Network Service, is a network protocol used by OMRON PLCs over different physical networks like Ethernet, Controller Link, DeviceNet, and RS-232C.

[Explore OMRON FINS](https://www.shodan.io/explore/category/industrial-control-systems)

**Crimson**

The protocol the Crimson V2.0 desktop software uses when communicating with the Red Lion Controls 3385 ASCII human machine interface (HMI).

[Explore Crimson v2](https://www.shodan.io/explore/category/industrial-control-systems)
Only 15% of seafarers had received any form of cyber security training.

Only 33% of seafarers said the company they last worked for had a policy to regularly change passwords on board.

71% of seafarers are willing to share personal data to further their career prospects.

52% are willing to share personal data in return for free Internet access.

50% of seafarers are willing to share their employment reviews, whilst 44% are prepared to share their medical history, with prospective employers.

According to Crew Connectivity 2018 Survey Report by Futurenautics group
PEOPLE ARE THE KEY
IT IS NOT ONLY ABOUT PROCESS AND TECHNOLOGY

PEOPLE
- Training & awareness
- Professional skills & qualifications
- Written procedures
- Authorizations
- Physical security

PROCESS
- Management Systems
- Governance Frameworks
- Policies & procedures
- Vendor/third party contracts-follow up
- Audit regimes

TECHNOLOGY
- System design, design review
- Software configurations
- Inspection/verification
- Testing
  - Functional testing
  - Vulnerability scanning
  - Penetration test
How can we in loss prevention help?

Make the crew see the cyber risk to stop it
WE HAVE IDENTIFIED SOME THREAT SCENARIOS FOR THE SHIP AND CREW TO BE AWARE AND LEARN FROM

Social Engineering
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.
Do they know the cyber risks?
REMOVABLE MEDIA / EXTERNAL HARDWARE & MIXING ISOLATED AND OPEN NETWORKS
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 network.
TAMPERING WITH NAVIGATION SYSTEMS & RANSOMWARE
THREAT SCENARIO #4

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 doesn’t require access to the vessel’s network or internal systems.
THREAT SCENARIO #5

RANSOMWARE

Ransomware encrypt files on a computer and demand that you pay to unlock your files.

Once the malicious software has infected one computer, be it personal or company computers, it may spread to others connected to the same network, quickly making it impossible to perform common tasks.
Think before you click!
CASE STUDY
CYBER SECURITY - SAFETY OF THE CREW

• Divide into groups

• Study the case background and incident text

• Perform an onboard risk assessment of the incidents and identify the factors which lead to it

• Use the keywords provided for your discussion
MAIN LEARNING POINTS
CREW PREPAREDNESS

1. Think and ask 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!
LOSS PREVENTION AWARENESS CAMPAIGNS
SUPPORT OWNERS AND OPERATORS IN THEIR DAY TO DAY OPERATIONS

ENCLOSED SPACE ENTRY
August 2018

CYBER SECURITY AWARENESS
in the Maritime Industry
May 2018

WATERTIGHT DOORS AWARENESS
April 2017

ANCHOR AWARENESS
January 2017
Connect with Gard on:

@GardGroup  @gard_insurance  Gard AS