



WHEN TRUST MATTERS

Case studies of cyber incidents onboard a Vessel



Vijay, Principal Consultant - Industrial Cybersecurity
Vijayan.Manogara@dnv.com / +65 96427273



Our purpose

To safeguard life,
property, and the
environment

Our vision

A trusted voice
to tackle global
transformations

Cyber Security key in DNV's Purpose and Vision

DNV Cyber Security Unit

- Based in Singapore, Norway(HQ), Netherlands, UK, Germany, France
- Across DNV globally: ~ 800 cyber security professionals
- Deep domain knowledge in Maritime, Oil & Gas and all target industries
- Access to local entities in 100+ countries
- Focus on critical infrastructure and CS for industrial control systems
- Wide range of customers across its market segments

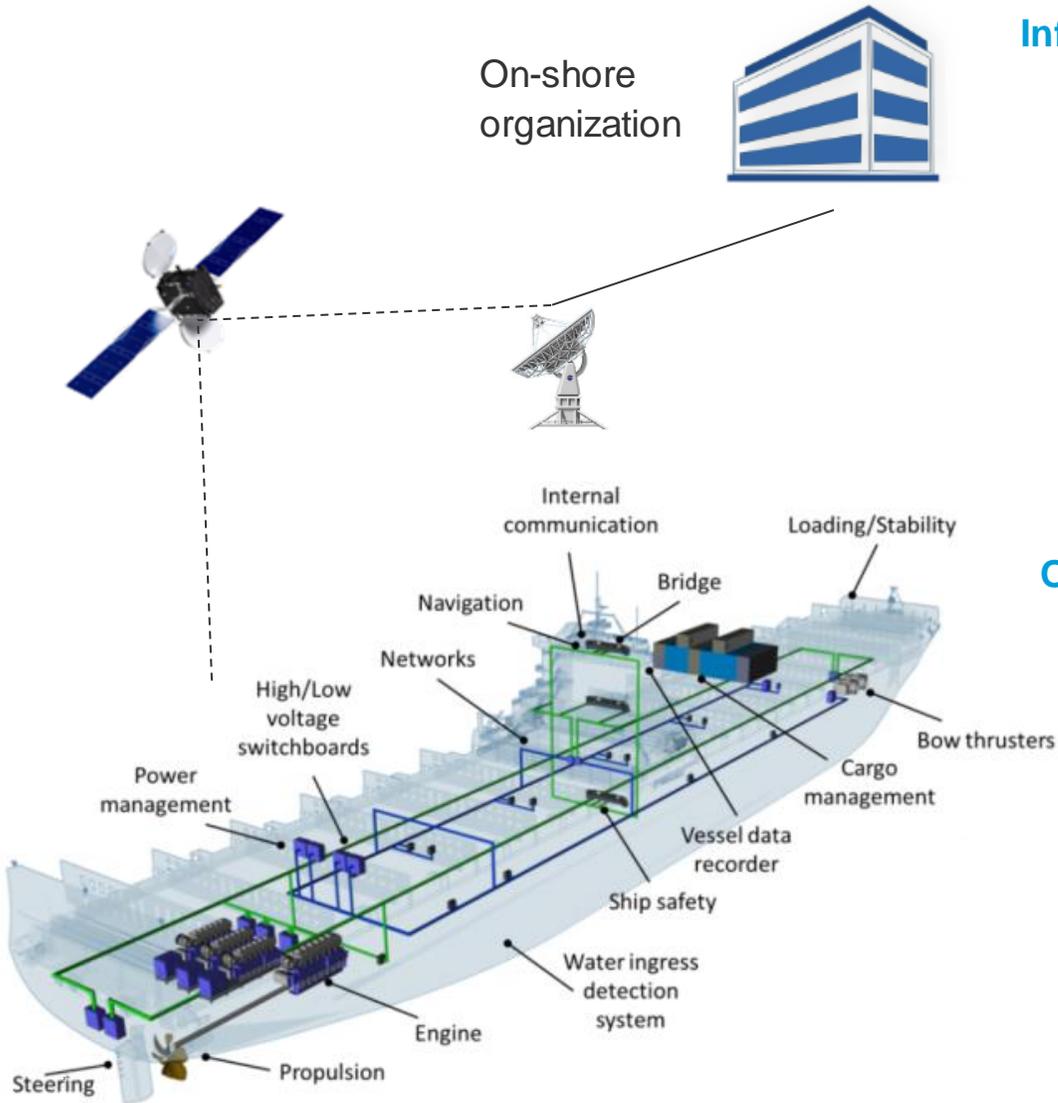
Cyber Security Certifications



DNV offices around the world



Safety in shipping today heavily depends on cyber systems



Information Technology (IT)

- Administration, accounts, crew lists, etc.
- Planned maintenance
- Spares management and requisitioning
- Electronic manuals and certificates
- Permits to work
- Charter party, notice of readiness, etc.

Operation Technology (OT)

- PLCs, SCADA
- On-board measurement and control
- ECDIS, GPS
- Remote support for engines
- Data loggers
- Engine and cargo control
- Dynamic positioning, etc.

At risk:

Mainly
finance
and
reputation

At risk:

Life, property
& environment
+
all of the
above

An aerial view of an offshore oil rig engulfed in a massive fire. Thick, dark black smoke billows upwards from the center of the inferno, partially obscuring the rig's structure. The rig's metal framework, including platforms and ladders, is visible against the smoke. The surrounding sea is dark and calm. The overall scene is one of a major industrial disaster.

How an hacker can cause an cyber incident?

Princess Cruises and Holland America data hacks!



Princess Cruises and Holland America Line announced this week that hackers gained access to personal information such as passport and Social Security numbers of guests, crew and employees.

Earlier this week, Carnival Corp. — the parent company of Princess and Holland America cruises — reported that hackers gained unauthorized access to some employee email accounts between April 11 and July 23, 2019. Those accounts contained the personal data of those who travel and worked on-board the Princess and Holland America ships, exposing a wide range of data, including:

- Names
- Addresses
- Social Security numbers
- Government identification information, such as passport numbers or driver's license numbers
- Credit cards and financial account information
- Health-related information

Carnival did not disclose how many passengers and employees were affected by the data breach and did not respond to CNBC Make It's request for comment. But the cruise company did file a [data security notice with the California Attorney General](#), which indicates at least 50 California residents were involved because that is the minimum number of people needed to trigger a mandatory filing.

<https://www.infosecurity-magazine.com/news/carnival-cruise-lines-hacked/>

At risk:

Mainly
finance
and
reputation

I read such news all the time!

What can I do about that ?

There can be two actionable steps you can take to help prevent cyber-attacks.

- **Security assessment:** locate issues and vulnerabilities and provide solutions.
- **Encryption:** Especially business details, files and personal information

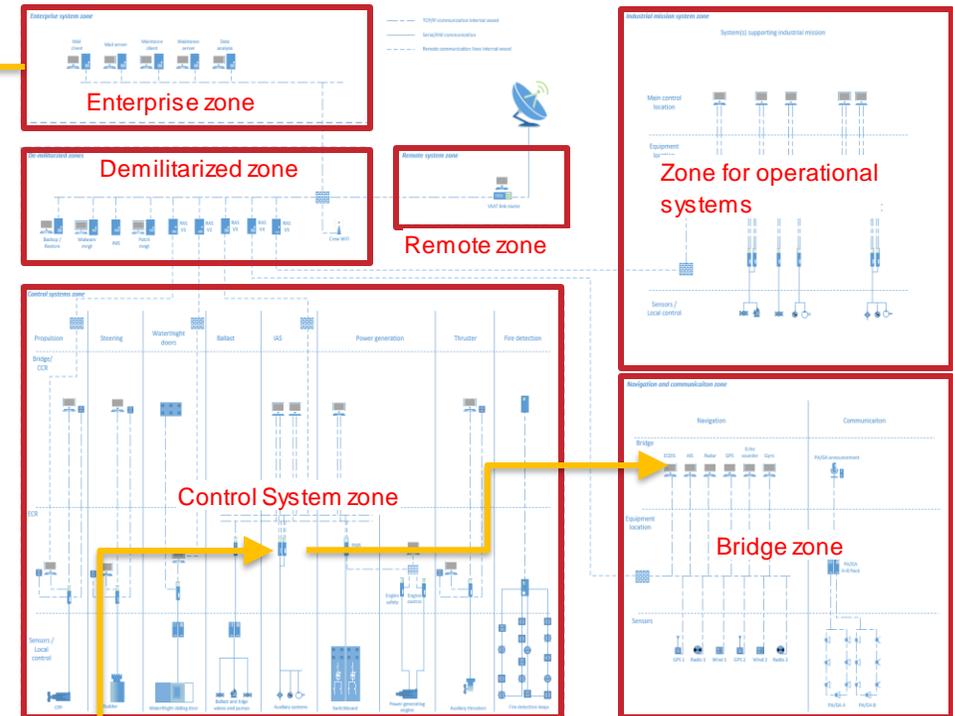
Actual event : when a cyber incident hits a cruise ship..

At risk:
Life, property
& environment

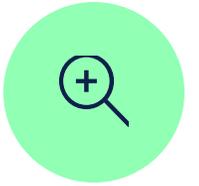
1. Crew onboard used the Engineering laptop, previously connected to the IT systems and then to OT systems – infected the Automation System...
 - The Automation System allows cost saving by allowing smaller crew size
2. Due to insufficient segregation malware propagated to Bridge Navigation systems
3. Crew had to manually control equipment
 - This operation normally requires much larger crew
 - Fuel pumps, lubrication, monitoring, etc.
4. Consequences
 - Cruise trip cut short and return to port
 - Tug(s) called in for safety
 - Vendor investigation team flown in from Europe the same day
 - Next trip also cancelled:
3500 passengers' times 2: refunds, hotels, travel, lost revenue, etc.



5. Total estimated cost = 35 – 210 MUSD



Incident response & investigation



- Understand what went wrong,
- What you need to do to recover effectively and
- Establish robust procedures for handling cyber attacks.

Key services you would need to think about/ Enable!



How DNV can help

- Identify the flaws in people, processes or technology that led to a cyber incident
- Recover efficiently from an attack
- Address the cyber gap between OT and IT systems and prevent incidents from happening again
- Develop incident response procedures and training programs.

It doesn't happen to me/ Wait & see approach!

- Ignorance of risks
- Compliance and regulation
- Personal and financial loss
- Social engineering

Iran-linked DEV-0343 hacking group targeting Defense, GIS, and maritime sectors (October 11, 2021)

Victims: Global maritime transportation companies with presence in the Middle East, regional ports of entry in the Persian Gulf, Several maritime, cargo transportation companies. US, Israeli defense technology companies

- TTP's: password sprays (O365), TOR proxy ip's, emulating Firefox in the user agent
- IOC's: extensive inbound traffic from TOR ip's in password sprays, emulation of Firefox and Chrome, enumeration against activesync and autodiscover endpoints (Exchange)

Password spraying is an attack that attempts to access a large number of accounts (usernames) with a few **commonly used passwords.**

Traditional brute-force attacks attempt to gain unauthorized access to a single account by guessing the password.

<https://www.microsoft.com/en-us/security/blog/2021/10/11/iran-linked-dev-0343-targeting-defense-gis-and-maritime-sectors/>

TTP: Tactics, Techniques, Procedures

GIS: Geographic information systems

IOC: Indicator of Compromise

Example of a “compliance” cyber incident, in 2022

Source: undisclosed.

- USCG inspectors go onboard a ship in 2022, **to inspect the ship according to IMO regulations**, including cyber risk management
- **Inspectors discover passwords noted on post-its** and attached to the automation screens
- **A cyber incident is declared, and the ship is detained by the authorities until remediation actions** (remedial training, installation of password management tools, change of passwords) have been performed and demonstrated to the satisfaction of the authorities.
- Impact: **loss of revenue during detainment**,
- **loss of trust by said authorities**
- and **High management attention** on the cyber risk at sea.



Insufficient control can lead to exposure. Take a holistic approach!



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



- Management systems and Governance
- Policies and procedures
- Risk and vulnerability management
- Supply chain security management
- Incident response
- Audit and reviews



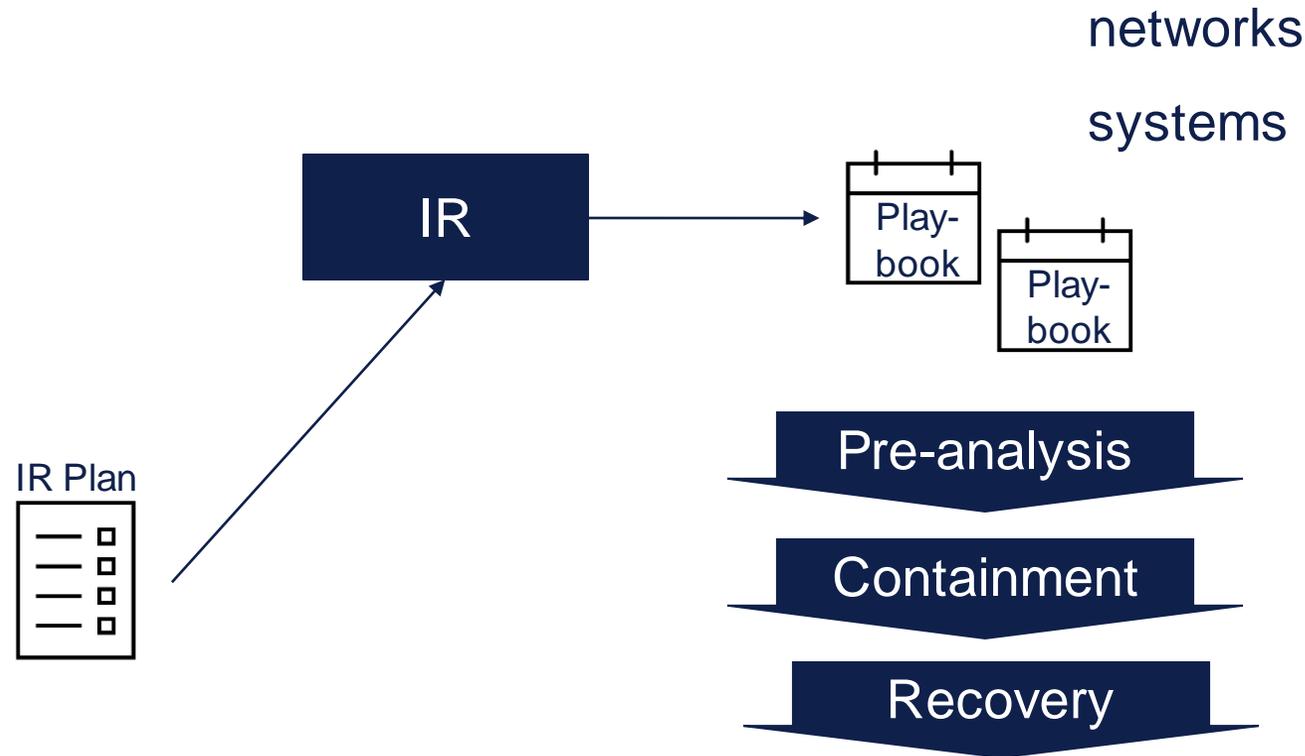
- System and network design
- Endpoint protection
- Software configuration
- Encryption protocols
- Detection and monitoring





Bravo!!!
You have survived so far!

Responding to Maritime Cyber Threats and Incidents



- Identify and discuss cyber events for a ship – threat model
 - Where do they appear – what are the largest uncertainties and risks
 - Where is need for support largest
- Need for support when an event occur
 - On board
 - On shore
 - Interface IT/OT
- Cooperation and communication with ship personnel
 - Realistic interaction with IR staff
 - Additional requirements to manage event
 - Critical systems that can't be tempered with
- Service delivery and value proposition

What has happened?

- What have you observed?
- Name of people that have been involved or affected by incident?
- What is not working?
- Is it an IT problem, or a control system/maritime system problem, or both? (checkboxes with a single line for a comment)
- Do you have any initial documentation for our analysts to review? (screen shots, computer logs, e-mails, links to web pages, ip addresses)

What has been done so far?

- What actions have been taken to identify or limit the problem?
- Who is the main contact person for the incident?

What evidence do you have that our analysts can start working with?

- Screenshots
- E-mails with suspicious links, etc.
- Links or IP addresses
- Computer logs
- Security system alerts

All evidence should be uploaded to our collection folder on Azure if possible.

Challenges for an Maritime cyber treat and incident handling

Cyber Security Incident response team(CSIRT)

- How to staff support with expertise for a service that must be available 24/7 but rarely used?
- Who is responsible for the Cyber Security team availability, competence development and performance?
- How to operate together with the Maritime CSIRT team ?

Competitive market where we need to find the niche

- Industrial OT
- Data analytics/AI
- Industrial MDR

Services

- Differentiate online/offline ships
- Data Direct Access to an expert
- Service descriptions and how to promote to potential shipowners

Business case

- Value proposition – reduced insurance premium for shipowners? Reduced risk for insurance companies?
- Ships/OT compared to IT in the management company

Commercial

- Who owns the contract with the shipowner?
- Who is going to sell the service and how?

Challenges to think through....

How to forward e-mails as attachments (to capture full headers)

How to upload files to our collection drive (use SharePoint/OneDrive, etc?)

How to export computer logs from Windows and Linux, and what logs to export.

PowerShell and bash scripts that they can run from a USB drive for initial artefact collection.

Playbook examples

One key point to convey is that most times for existing vessels the OT infrastructure is **not connected via TCP/IP**. so most OT incidents cannot be detected with the help of monitoring.

A very limited degree of our customers have that in the OT network, but it is common in the IT infrastructure.

The vessels of today is highly dependant on **the vigilance of the crew** to notice strange behaviour of the systems to identify cyber incidents.

Incident Response Playbook – Beaconing

OT: Unauthorized firmware change

	Treatment artefacts	Prerequisites
Inputs:	OT IDS alert	Network based OT IDS in place Known versions of firmware to be used
Outputs:	Confirmed affected devices Extracted unauthorized firmware	Asset inventory required for ID
Description:	Identify affected devices. Confirm firmware version detected is correct and deviates from intended version. Secure firmware download if possible as evidence and forensic analysis. Recover to intended firmware version if required.	

Step	Collect	Analyze and Take Action
PAI	Set up OT IDS that can detect firmware versions based on packet capture. Maintain asset inventory with firmware versions. Create alarms on firmware version mismatch.	Be prepared to correlate firmware related alarms with other artefacts that could indicate malicious activity.
CSA	IDS alert showing wrong firmware version is detected. If possible, collect firmware from device.	Verify that the alert is correct by connecting to the device if possible. Extract firmware on device for further analysis if possible.
CCP	Compromised computers	Check for artefacts indicating further compromise, including paths for an attacker to achieve control over suspicious device. Reinstall approved firmware if required. Discuss with assistance and vendor representative if it is unclear which version should be installing.
AA	List of affected machines and accounts	Create report of incident handling Initiate investigation of devices in same network segment to identify further compromise. Update detections as relevant (see threat intel feed integration).

Useful tools: IDS, datasheets, service computer with software to update OT equipment

Incident Response Playbook – Phishing

Phishing

	Treatment artefacts	Prerequisites
Inputs:	E-mail headers, IP addresses, URLs	E-mail samples (user report, spam filter, etc)
Outputs:	Identified domains, identified accounts, identified payloads, identified devices, blocked CS, cleaned devices, remediated accounts	URL and IP threat intelligence, searchable e-mail logs, firewall rule updates, endpoint protection updates, account management access

Step	Collect	Analyze and Take Action
PAI		Clear analysis across for e-mail logs/security tooling Train users to report suspected phishing e-mails Set up system to block known malicious senders (e-mail)
CSA	Phishing report Obtain e-mail headers (envelope from), received (ip address), from subject. Collect from body URL's, ip addresses, attachments, instruction messages.	Set up system to block against malicious senders (firewall, DNS, endpoint protection) Check URL and IP addresses against threat intelligence Execute URL in a sandbox Check sender domain and ip addresses against threat intelligence Hash attachment file (SHA-1) and check against threat intelligence
CCP	Compromised computers	Classify as CEO fraud, credential theft, malware download, information elicitation, other. Take positive. Determine accounts and hosts that could be affected.
AA	List of affected machines and accounts	If CEO Fraud: (1) Contact victims, interview about actions taken. If credential compromise: (1) Check DNS logs for redirects indicating compromise of credentials, (2) Talk to victims for more details. (3) Reset any potentially compromised credentials. If malware download: (1) Run AV scan on potentially infected host device. (2) Obtain IDS from malware sample and check environment for signs of infection. Continue to PLAYBOOK/ANNEX if required.
CCP	List of affected accounts List of affected devices	Accounts: Search for potential abuse in case of expanded blast radius. Reset passwords if not done. Devices: Check logs for IOC's.
AA	List of affected accounts List of affected devices	Disable to PLAYBOOK/ANNEX if necessary. Create report of incident handling Update detections as relevant Remind users about phishing awareness

Useful tools: urlscan.io, virustotal.com

DNV's cyber security services



Strategy & Programme

Develop effective cyber security strategies and programmes, even when you face tight deadlines



Testing & Verification

Test and verify the resilience of systems, networks and components, and access practical, unbiased advice to enable you to prioritize mitigation of vulnerabilities



Safety & security risk management

Ensure security and safety in the design of new and existing projects



Governance, risk & compliance

Implement robust governance, risk, and compliance strategies across projects and operations



Incident response & investigation

Understand what went wrong, what you need to do to recover effectively and establish robust procedures for handling cyber attacks



Insights & training

Ensure that you have the right insights and training in place to build awareness across the full life cycle of your operations

About DNV - Maritime

DNV is the world's leading classification society and a recognized advisor for the maritime industry. We enhance safety, quality, energy efficiency and environmental performance of the global shipping industry – across all vessel types and offshore structures

<https://www.dnv.com/about/maritime/index.html>

SAFEGUARD LIFE, PROPERTY AND THE ENVIRONMENT

Vijayan.Manogara@dnv.com

+65 96427273

www.dnv.com

