Cyber Security in the shipping industry

Capital Link Cyprus Shipping Forum
“We are vulnerable in the military and in our governments, but I think we're most vulnerable to cyber attacks commercially. This challenge is going to significantly increase. It's not going to go away.”

Michael Mullen - US Navy Admiral
Chairman of the Joint Chiefs of Staff
Maritime is not an exception
Vessel Digitization
Transforming the shipping industry
Entering the digitization era

- Computerized systems will transform the shipping industry
- Smart – autonomous or even automated ships

Rolls Royce already entered the game with the Autonomous Waterborne Applications Initiative (AAWA)

2020
Reduced crew with remote support and operation of certain functions

2025
Remote controlled unmanned coastal vessel

2030
Remote controlled unmanned ocean-going ship

2035
Autonomous unmanned ocean-going ship

Autonomous Ship Technology Symposium 2016 - Amsterdam
Vessel Digitization
Vessels Security Challenges

Vessels interconnection means more exposure to the world wide web
Vessels Security Challenges

- Data at Rest
- Data in Transit
- Intelligence
- Crew Turnover
Electronic Chart Display & Information System (ECDIS)
ECDIS Systems

- Geographic information systems
- International Maritime Organization compliant
- Alternative / compliant to paper nautical charts
- Can be interfaced with NavText and AIS
- July 2018 – Mandatory for all vessels in international voyages.
Attacking ECDIS Systems

- ECDIS systems are in essence desktop PCs
- With physical access a malicious person could use the USB slot to load incorrect/outdated maps, access the underlying operating system or spread malware/ransomware.
Attacking ECDIS Systems

- As with any other PC, ECDIS systems can be tampered with.
- A number of these systems run with administrative rights and no password protection.
Automatic Identification System (AIS)
AIS Systems

- Automatic tracking system for identifying and locating vessels
- 2002 – First mandate for vessels over 300GT to be equipped with a Class A type AIS transceiver.
- AIS information supplements marine radar, which continues to be the primary method of collision avoidance for water transport.
- Aid in accident investigation and in search and rescue operations.
- The information is also sent to providers such as Maritimetrack.com, Vesselfinder.com or Aishub.net.
- Transmit in the Marine bands - Channel A 161.975 MHz (87B) & Channel B 162.025 MHz (88B)
AIS Systems Messages

AIS can send up to 27 types of messages

- Message 18 is sent between anywhere 30 seconds and 3 minutes to report the vessel's position.
- Message 14 is a safety related broadcast used in emergencies.
AIS Systems Risks

- AIS communications do not employ authentication or integrity checks.
- Communication is made over RF
- Anyone with a cheap RF receiver can also “listen” to these messages. (Range dependent)

Maritime security - AIS ship data

At its 79th session in December 2004, the Maritime Safety Committee (MSC) agreed that, in relation to the issue of freely available automatic information system (AIS)-generated ship data on the world-wide web, the publication on the world-wide web or elsewhere of AIS data transmitted by ships could be detrimental to the safety and security of ships and port facilities and was undermining the efforts of the Organization and its Member States to enhance the safety of navigation and security in the international maritime transport sector.

The Committee condemned the regrettable publication on the world-wide web, or elsewhere, of AIS data transmitted by ships and urged Member Governments, subject to the provisions of their national laws, to discourage those who make available AIS data to others for publication on the world-wide web, or elsewhere from doing so.

In addition, the Committee condemned those who irresponsibly publish AIS data transmitted by ships on the world-wide web, or elsewhere, particularly if they offer services to the shipping and port industries.

Because of maritime laws and best practices, everyone needs to address this type of an alert.

**Arbitrary weather forecast**
Hackers impersonate actual issuers of weather forecast such as the port authority and arbitrarily change the weather forecast delivered to ships.

**AIS Spoofing**
Hackers can send specially crafted messages that could mimic the location of an existing vessel, or even create a fake vessel and place it on its own virtual course.

**Fake CPA**
Hackers create a fake CPA (closest point of approach) alert.

**Replay Attacks**
Hackers capture and store AIS data and replay spoofed messages in specific timeframes.

**Ship Hijacking**
Hackers download the data of an existing ship, changing some of the parameters and submitting it to the AIS service.

**Man-in-the-water**
Because of maritime laws and best practices, everyone needs to address this type of an alert.
AIS Systems Attacks

Even via RF the hackers have 4 attack vectors

- AIS Gateway
- Vessel Traffic Service
- Vessels
- Offshore
An exaggerated example?

1. 300 ton ships should not drive down the main street of a city
Deloitte’s Threat Analytics
AIS Systems Verified Attacks

- Modification of all ship details such as position, course, cargo, flagged country, speed, name & MMSI
- Creation of fake vessels e.g. having a vessel with nuclear cargo show up off the coast of the US
- Create and modify Aid to Navigations (AToN) entries, such as buoys and lighthouses.
- Research has been published in 2013 but since then there was not an improvement on the protocol
- ITU Radiocommunication Sector (ITU-R); the developers of the AIS standard and the protocol specification have acknowledged the problem
It’s not all bad...

Reliance on crew
- Sufficient and continuous training on Cyber Security
- Development of a Cyber Security Policy

Reliance on manual controls
- Crew
- Paper Charts
- Radar

Vessels must be treated as any other network
- Security Audits
- Penetration Testing
- Physical Security Assessments

Incident Response
- Development of Contingency Plans
- Stress Tests
To be effective and well balanced, a cyber program must have three key characteristics: secure, vigilant, and resilient.

**Being SECURE**
means having risk-prioritized controls to defend critical assets against known and emerging threats.

**Being VIGILANT**
means having threat intelligence and situational awareness to anticipate and identify harmful behavior.

**Being RESILIENT**
means being prepared and having the ability to recover from cyber incidents and minimize their impact.
Maritime Industry is based on IT solutions with global interfaces to improve efficiency and international networking. Technical dimensions of shipping and of ships themselves are not depending on technology only for communication purposes. The progress of information technologies will definitely proceed and as a logical consequence, turn into complex risk-scenarios which currently seem to be difficult to be solved.

Balance people, processes and technology. Information security is not just about computer security. Computer security can carry the wrong assumption that as long as the infrastructure and systems are secure, the organization is also secure. You have to invest in all core elements of information security: physical, human and cyber.

Act as you have already been hacked. Breaches occur at all organizations – not because they are badly managed, but because hackers and cyber-criminals are getting smarter every day. Although it isn’t possible for any organization to be 100 percent secure, it is entirely possible to use a mix of processes for prevention, detection and response to keep cyber-risk below a level set by the board and enable an organization to operate with less.

Four takeaway questions to reflect on through the lens of a secure, vigilant, and resilient approach to cybersecurity:

1. **Are we focused on the right things?** Often asked, but difficult to accomplish. Understand how value is created in your organization, where your critical assets are, how they are vulnerable to key threats. Practice defense-in-depth.

2. **Do we have the right talent?** Quality over quantity. There may not be enough talent to do everything in-house, so take a strategic approach to sourcing decisions. Are the security teams focused on the real business areas?

3. **Are we proactive or reactive?** Retrofitting for security is very expensive. Build it upfront in your management processes, applications, and infrastructure.

4. **Are we adapting to change?** Policy reviews, assessments, and rehearsals of crisis response processes should be regularized to establish a culture of perpetual adaptation to the threat and risk landscape.
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte has in the region of 200,000 professionals, all committed to becoming the standard of excellence.

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this publication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.