



Cybersecurity incident reporting: current requirements in EU law and at IMO

EMSA Maritime Cybersecurity Conference 2024, Lisbon

Edward Banks, Policy Officer, DG MOVE A5 (Security Unit)

3 October 2024

1. EU Maritime Security Legislative Framework
2. IMO provisions on cybersecurity incident reporting
3. Potential future developments

1. EU Maritime Security Legislative Framework

EU Maritime Security Legislation

- The International Ship and Port Facility Security (ISPS) Code as the basis
- Regulation (EC) N°725/2004 on enhancing ship and port facility security
- Directive 2005/65/EC on enhancing port security
- Cover port, port facility and ship security
- Compliance monitoring through both Commission inspections and inspections by Member States
- The legislation refers to assets and infrastructure that need to be protected, such as “computer systems and networks” – both for ships and port facilities

Ships unaffected?



- Some ships have few digital tools onboard
- However shipping, like other sectors, is becoming increasingly digitalized
- We want to avoid any incident involving threats to physical wellbeing of people, or blockage of important waterways
- Suez Evergreen incident not due to cyber, but what if?

Incident reporting in MarSec legislation



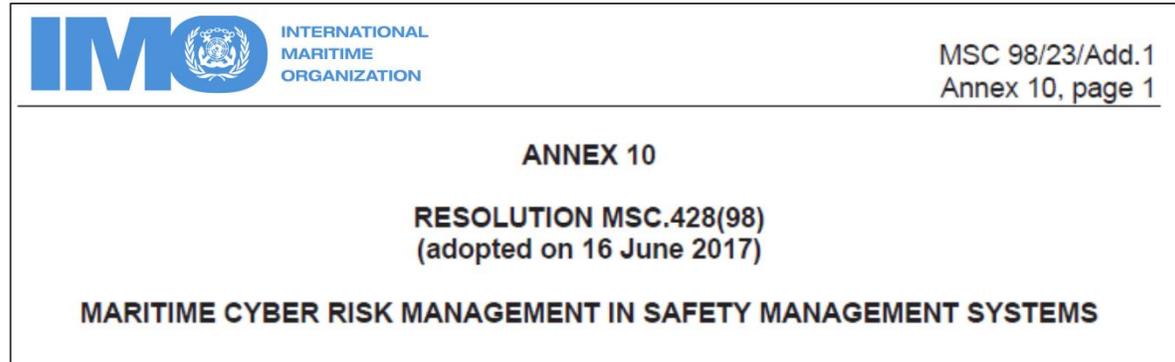
- “Security incident means any suspicious act or circumstance threatening the security” of a ship/ port facility
- Security plans must set out the procedures for reporting security incidents
- We expect that incidents, in particular repetitive or important incidents, lead to a review of the security procedures in place

NIS2 Directive on incident reporting

- An incident means “an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information system”
- Article 23 on reporting obligations
- Notification without undue delay of “significant incidents” to MS CSIRT
- Applicable to shipping companies, port and port facilities that fall under the scope of the Directive, but not to individual vessels

2. IMO provisions on cybersecurity incident reporting

Resolution MSC.428(98)



- The IMO encourages Administrations “to ensure that cyber risks are appropriately addressed in safety management systems”
- So cyber risk management for ships should be addressed through the ISM Code
- But there was also an agreement at MSC 101 that reference be made in the Ship Security Plan (ISPS Code) to cyber risk management procedures found in the Safety Management System (ISM Code)

IMO Guidelines on cyber risk management



IMO INTERNATIONAL
MARITIME
ORGANIZATION

E

4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telephone: +44 (0)20 7735 7611 Fax: +44 (0)20 7587 3210

MSC-FAL.1/Circ.3
5 July 2017

GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

1 The Facilitation Committee, at its forty-first session (4 to 7 April 2017), and the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), having considered the urgent need to raise awareness on cyber risk threats and vulnerabilities, approved the *Guidelines on maritime cyber risk management*, as set out in the annex.

2 The Guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.

3 Member Governments are invited to bring the contents of this circular to the attention of all stakeholders concerned.

4 This circular supersedes the interim guidelines contained in MSC.1/Circ.1526.

At its 107th session, the Maritime Safety Committee (MSC) agreed to include in the provisional agenda of MSC 108 an output on "Revision of the Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3/Rev.2) and identification of next steps to enhance maritime cybersecurity", with a target completion year of 2024

Incident reporting in the draft revised IMO guidelines

- Cyber incident “means an occurrence or a sequence of occurrences, which actually or potentially results in adverse consequences to a CBS or to the information that they process, store or transmit, and which may require a response action to mitigate the consequences”
- Detect a cyber incident in a timely manner
- Report incidents to necessary parties within required timeframes as defined by Administrations
- Carry out root cause analysis of cyber incidents, with the objective of resolving underlying issues

What might be missing?

- The IMO Guidelines on Maritime Cyber Risk Management remain recommendatory
- No common agreed format for reporting cyber incidents on ships



3. Potential future developments

Future steps at IMO

- Upcoming MSC 109 – USA proposal to further develop cybersecurity standards for ships and port facilities and establish a working group at MSC 110, with strong backing from a number of countries
- Still to be defined what further standards will be proposed – submissions will have to be made to MSC 110
- More recommendations on follow-up of cyber incidents? A common reporting format?

THE WHITE HOUSE

Administration Priorities The Record Briefing Room Español MENU

FEBRUARY 21, 2024

Executive Order on Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States

BRIEFING ROOM › PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, including section 1 of title II of the Act of June 15, 1917, as amended (46 U.S.C. 70051) (the "Act"), and in addition to the finding in Executive Order 10173 of October 18, 1950, and any other declaration or finding in force under section 1 of the Act, I find that the security of the United States is endangered by reason of disturbances in the international relations of the United States that exist as a result of persistent and increasingly sophisticated malicious cyber campaigns against the United States, and that such disturbances continue to endanger such relations, and hereby order that:

What the USA is doing

- Executive Order with different measures, including reporting requirements for an actual or threatened cyber incident
- Proposed rules for US flagged vessels and US port facilities
- Different Circulars, with one on incident reporting (NVIC 02-24)

Information sharing within the EU

- One notable advantage of increased reporting of cyber incidents would be a greater awareness of threats by national authorities
- Sharing of this information within the EU could help raise preparedness, but sensitive information has to be protected
- Measures are in place through NIS2, but what about individual vessels?



Conclusions



- Existing provisions on incident reporting through EU legislation and at IMO
- There may be further developments at IMO
- Information sharing can be key in raising awareness and preparedness

Thank you



© European Union 2020

Unless otherwise noted the reuse of this presentation is authorised under the [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/) license. For any use or reproduction of elements that are not owned by the EU, permission may need to be sought directly from the respective right holders.

