

# Cyber Threats: Reviewing and updating your Port Facility Security Assessment


## Part B Agenda Item 5

**Luca GARGANO:** Project Officer for Maritime Security

**Ruben PANES:** Project Officer for Port State Control and Environment.

Lisbon / 26<sup>th</sup> November 2019

15.3 A PFSA should address the following elements within a port facility:


- .1 physical security;
- .2 structural integrity;
- .3 personnel protection systems;
- .4 procedural policies;
-  .5 radio and telecommunication systems, including computer systems and networks;
- .6 relevant transportation infrastructure;
- .7 utilities; and
- .8 other areas that may, if damaged or used for illicit observation, pose a risk to persons, property, or operations within the port facility.

**MANDATORY**

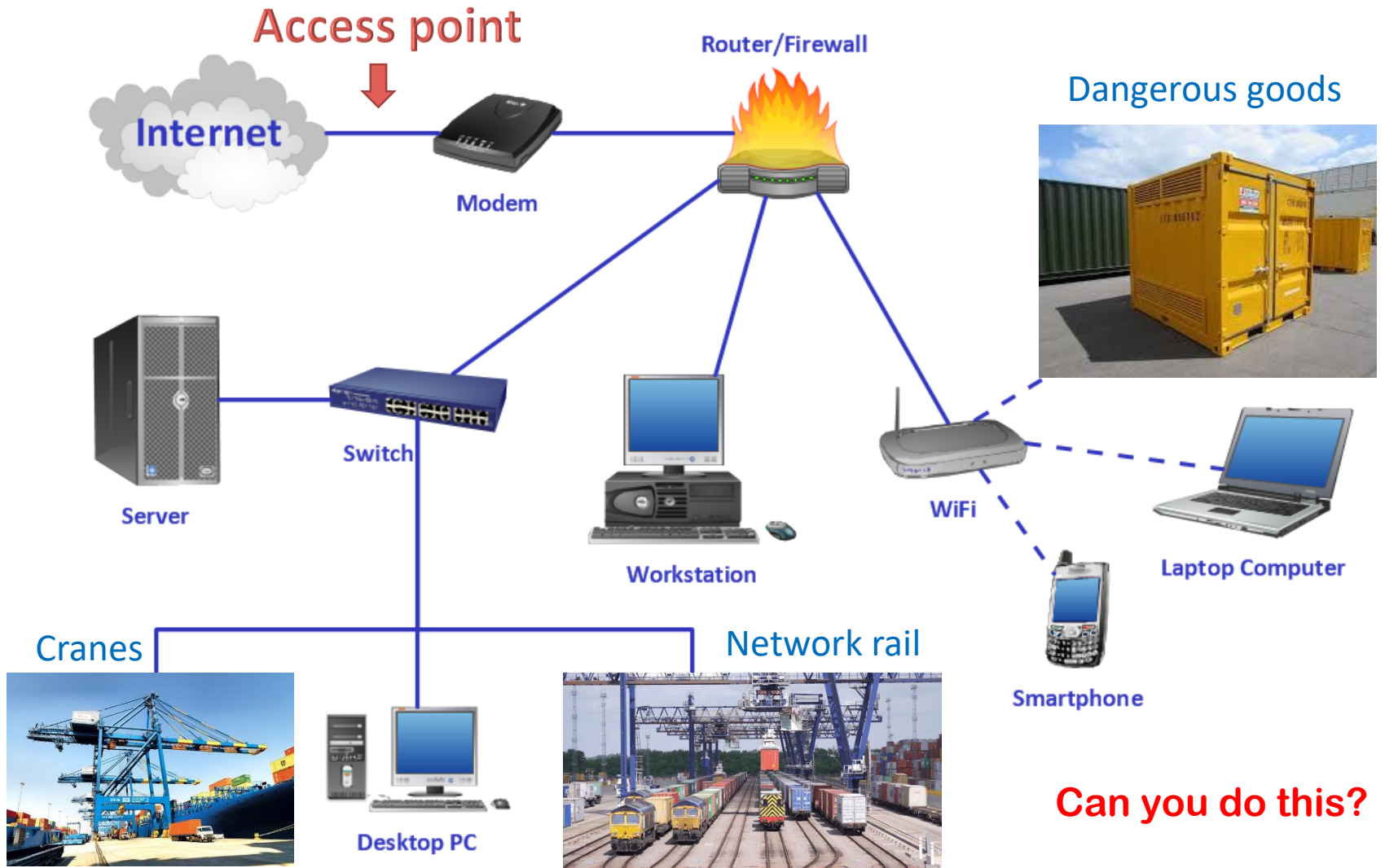
15.5 The port facility security assessment shall include, at least, the following elements:

- .1 identification and evaluation of important assets and infrastructure it is important to protect;
- .2 identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritise security measures;
- .3 identification, selection and prioritisation of countermeasures and procedural changes and their level of effectiveness in reducing vulnerability; and
- .4 identification of weaknesses, including human factors, in the infrastructure, policies and procedures.

15.7 Assets and infrastructure that should be considered important to protect may include:

- .1 accesses, entrances, approaches, and anchorages, manoeuvring and berthing areas;
- .2 cargo facilities, terminals, storage areas, and cargo handling equipment;
-  .3 systems such as electrical distribution systems, radio and telecommunication systems and computer systems and networks;
- .4 port vessel traffic management systems and aids to navigation;
- .5 power plants, cargo transfer piping, and water supplies;
- .6 bridges, railways, roads;
- .7 port service vessels, including pilot boats, tugs, lighters, etc.;
- .8 security and surveillance equipment and systems; and

# Network mapping



15.4 Those involved in a PFSA should be able to draw upon expert assistance in relation to:

- .1 knowledge of current security threats and patterns;
- .2 recognition and detection of weapons, dangerous substances and devices;
- .3 recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;
- .4 techniques used to circumvent security measures;
- .5 methods used to cause a security incident;
- .6 effects of explosives on structures and port facility services;
- .7 port facility security;
- .8 port business practices;
- .9 contingency planning, emergency preparedness and response;
- .10 physical security measures, e.g. fences;



- .11 radio and telecommunications systems, including computer systems and networks;
- .12 transport and civil engineering; and
- .13 ship and port operations.

**MANDATORY**



## ISPS 15.5.4

Identification of weaknesses, including human factor, in the infrastructure, policies and procedures.

To be addressed in the PFSP





 [twitter.com/emsa\\_lisbon](https://twitter.com/emsa_lisbon)  
 [facebook.com/emsa.lisbon](https://facebook.com/emsa.lisbon)

 **EMSA**  
European Maritime Safety Agency