European Commission | Horizon 2020
European Union funding
for Research & Innovation

Cyber Security PPP: Addressing Advanced Cyber Security Threats and Threat Actors

Cyber Security Threats and Threat Actors Training - Assurance Driven Multi- Layer, end-to-end Simulation and Training

D1.1 The pilots' requirements analysis report[†]

Abstract: To demonstrate the use of the THREAT-ARREST framework for effective training against Cyber Attacks and evaluate and validate the proposed framework, we have defined and analyzed here a set of requirements in terms of training, threats analysis and security in high-risk organisations, with a special focus on the three fields of the proposed pilots. Furthermore, we defined the evaluation criteria and Key Performance Indicators (KPIs) that will be used for the evaluation of the pilots.

Contractual Date of Delivery	31/12/2018
Actual Date of Delivery	31/12/2018
Deliverable Security Class	Public
Editor	*Prof. Takis Varelas (DANAOS)*
Contributors	STS, B&B, TUBS, LSE, ARES
Quality Assurance	*Fulvio Frati (UMIL),* *George Hatzivasilis (FORTH)*

[†] *The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786890.*

The *THREAT-ARREST* Consortium

Foundation for Research and Technology – Hellas (FORTH)	Greece
SIMPLAN AG (SIMPLAN)	Germany
Sphynx Technology Solutions (STS)	Switzerland
Universita Degli Studi di Milano (UMIL)	Italy
ATOS Spain S.A. (ATOS)	Spain
IBM Israel – Science and Technology LTD (IBM)	Israel
Social Engineering Academy GMBH (SEA)	Germany
Information Technology for Market Leadership (ITML)	Greece
Bird & Bird LLP (B&B)	United Kingdom
Technische Universitaet Braunschweig (TUBS)	Germany
CZ.NIC, ZSPO (CZNIC)	Czech Republic
DANAOS Shipping Company LTD (DANAOS)	Cyprus
TUV HELLAS TUV NORD (TUV)	Greece
LIGHTSOURCE LAB LTD (LSE)	Ireland
Agenzia Regionale Sanitaria Pugliese (ARES)	Italy

Document Revisions & Quality Assurance

Internal Reviewers

1. *Fulvio Frati, Stelvio Cimato, Elvinia Riccobene (UMIL)*
2. *George Hatzivasilis (FORTH)*

Revisions

Version	Date	By	Overview
0.7	18/12/2018	Julien Debussche	Input From B&B on Legal framework
0.6	16/10/2018	Menelaos Ioannidis	Input from LSE for Energy Pilot
0.5	06/12/2018	Jason Somarakis	Input from STS
0.4	05/12/2018	Marinos Tsantekidis	Added TUBS input
0.3	05/12/2018	Fulvio Frati	Input from ARESS for Health Pilot
0.2	20/11/2018	Editor	Input for Maritime Pilot
0.1	30/10/2018	Editor	First Draft

List of Abbreviations

EU: European Union
ISPS: International Ship and Facility Security Code
IMO: International Maritime Organisation
IT: Information Technology
OT: Operational Technology
AI: Artificial Intelligence
IoT: Internet of Things
ECDIS: Electronic Chart Display and Information Systems
GNSS: Global Navigation Satellite System
AIS: Automatic Identification System
VDR: Voyage data recorder
ARPA: Automatic radar plotting aid
VLAN: Virtual Local Area Networks
CTTP: Cyber Threat and training preparation
IDS: Intrusion Detection System
IPS: Intrusion Prevention System
VPN: Virtual Private Network
ICT: Information and communications technology
MQTT: Message Queuing Telemetry Transport
GDPR: General Data Protection Regulation
NISD: Network and Information Security Directive
KPI: Key Performance Indicator

Table of Contents

List of Figures

List of Tables

1 Introduction

To demonstrate the use of the THREAT-ARREST framework for effective training against Cyber Attacks, and evaluate and validate the proposed framework, real operational Cyber Systems will be used from three separate, distinct domains, namely smart energy (Pilot 1), healthcare (Pilot 2), and smart shipping (Pilot 3).

The selected pilots within these domains use different Cyber Systems platforms, and different types of smart objects, devices, and networks. They also involve end-users both of public (Pilot 2) and private organisations (Pilot 1 and Pilot 3) and cover a significant spectrum of different (in type, significance, and expected level of enforcement) security requirements, thus enabling a comprehensive evaluation of the THREAT-ARREST approach.

The content below includes a mapping of each complementary field of the THREAT-ARREST pilots to a specific security framework and requirements. In addition to the platform's system requirements analysis report (D1.2), this mapping feeds inputs to the definition of the THREAT-ARREST architecture and initial identification of the exact form of training and simulation models for the pilot scenarios and Cyber Systems, which constitutes one of the project's main objectives. Furthermore, we define evaluation criteria and Key Performance Indicators (KPIs) that will be used for the evaluation of the pilots.

This deliverable is part of WP1, which tackles the issues of the project platform's requirements and design. The main contribution is the definition and analysis of the basic requirements in terms of training, threats analysis, and security in high-risk organisations, with a special focus on the three fields of the proposed pilots Energy, Healthcare and Maritime), as well as the identification of the criteria and KPIs used to evaluate the pilots.

The rest of the document is structured as follows: in **Chapter 2** we describe the system of each of the pilot cases, analysing the architecture and infrastructure that will be used. **Chapter 3** offers details on the security framework and requirements of the pilots, carrying out a threat assessment, while at **Chapter 4** and **5** the laws and regulations surrounding the respective systems are referring the general and sectorial legal perspectives, respectively. In **Chapter 6** we define the evaluation criteria and KPIs that will be used for the evaluation of the pilots. **Chapter 7** concludes and links the deliverable content with other related tasks/deliverables.

2 Pilot system Definition

2.1 Smart Energy System

In this section we will take care of the description of the Smart energy system infrastructure by giving a short introductory definition of the system and following up with the description of system topology, vulnerabilities, networking and communication

2.1.1 Description

Lightsource Labs a new Energy ICT company provides robust and scalable hardware/software platforms, and applications connecting intelligent energy. Its end-to-end solutions serve markets, such as distributed energy monitoring and control (mainly solar and battery), smart appliances load management and electric vehicle charge management.

IoT based solutions are focused on the integration of distributed solar, energy storage, electric vehicles, and other energy resources on the grid. In parallel these distributed energy resources improve the balancing of the system and avoid expensive investments in grid infrastructure.

Any distributed generation asset or any consumption load can be smart enough to have control over their energy flow to match the power available into the grid and assist in helping to balance the system. The focus is to help achieve higher penetration of renewable energy sources, in particular distributed energy resources (DER) deployed behind the meter, at residential or commercial scale.

Lightsource Labs is developing a smart energy management solution for the residential sector by utilizing smart home technologies combined with solar generation, home batteries and electric vehicles. As time goes by, the concept of IoT widely spreads, which stands for Internet of things. All these smart boxes, light bulbs, shades, thermostats, voice assistants, and smart machines are slowly installed into households, businesses and industrial environments.

In order to control smart devices inside a household, an automated process is required, to manage connected devices and to have the ability to connect more smart devices in the future.

Thus, complex systems come into play which use communication protocols, so that several machines can "talk" with one another. By doing so, commands and data transmission is achieved. This creates the indispensable need that applications and systems make use of the internet of things (IoT) and the industrial internet of things (IIoT).

Looking over two of the most common IoT protocols for transferring messages (Hatzivasilis et al., 2018):

- **Message Queuing Telemetry Transport (MQTT)** is a communication protocol widely used in both IoT and IIoT deployments. MQTT is a publish-subscribe protocol that facilitates one-to-many communication mediated by brokers. Clients can publish messages to a broker and/or subscribe to a broker to receive certain messages. Messages are organized by topics, which essentially are "labels" that act as a system for dispatching messages to subscribers.
- **Constrained Application Protocol (CoAP),** on the other hand, is a client-server protocol that, unlike MQTT, is not yet standardized. With CoAP, a client node can command another node by sending a CoAP packet. The CoAP server will interpret it, extract the payload, and decide what to do depending on its logic. The server does not necessarily have to acknowledge the request.

The Message Queuing Telemetry Transport (MQTT) protocol as a communication protocol can connect, control and monitor all smart home devices. For the implementation of the MQTT protocol, a process must be followed. Users must establish a server. For customers, the server most often resides on a PC or a mini computer such as Raspberry Pi. That device will later on be used as an anchor for devices to connect to, but also communicate with each other. Even though the MQTT as a protocol is secure, if the implementation and configuration of it, is not correct, there is a risk of exposing severe security risks.

A recent research from Avast found that 49,000 MQTT servers are publicly visible on the internet due to a misconfigured MQTT protocol (AVAST, 2018). This includes more than 32,000 servers that had no password protection, putting these smart homes and businesses using such MQTT servers at risk of leaking data. If the MQTT protocol is not properly configured, cybercriminals can gain complete access to a home and for example, learn when their owners are at home, manipulate entertainment systems, voice assistants, household devices, and physically open smart doors.

2.1.2 System Architecture and Infrastructure

Lightsource Labs system develops a Distributed Generation System. Distributed generation refers to a variety of technologies that enable the supply of power at or near where it will be used - such as solar panels, batteries and electric vehicles. The structure of such a system is shown in Figure 1. These smaller scale assets are referred to as Distributed Energy Resources (DERs) and they are becoming increasingly cost effective and in-demand, evidenced by their sustained fall in price and recent acquisitions in the space. DERs create a more sustainable and cost-effective energy mix to consumers. Their expansion is being driven primarily by the cost competitiveness of solar and battery technologies. Similar to almost every industrial activity, the development of these has followed an exponential learning curve – as volume scales and knowledge builds, prices drop. While prices have not yet fallen to wholesale electricity price levels, DERs have other benefits such as reducing the need for expensive peaker plants, diminishing spend on new transmission and distribution lines and increasing the reliability of the energy network.

.

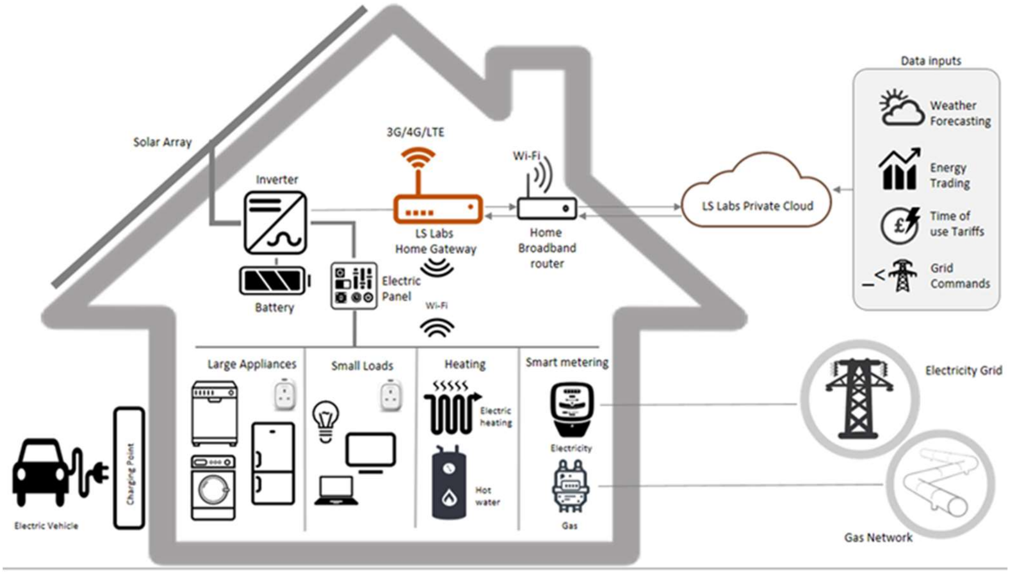


Figure 1. Example of a Smart Home-Distributed Generation System

As DERs become more prevalent, they present an opportunity to supplant traditional baseload generation - disrupting the structure of the energy industry value chain. One of the key opportunities to acquire revenue is in the home. By installing DERs in the household, residential consumers can generate, and store energy reducing their dependence on grid price variability and allow them to sell energy locally at select times. A connected community of homes could help facilitate this energy collaboration, communicating with each other and to the grid to identify the best times to buy, or sell, energy.

For solar developers, an area of focus is making installation pain-free and ensuring consumers are aware of the short and long-term benefits. DERs will change the position of 'winners' in the energy industry and the connected home will be a critical node in local, community and regional energy networks.

The reason IoT security is lacking is because the devices are built using technology protocols that date back to the 1980s. This is generally because the early use cases for IoT devices were largely industrial. There was high demand for systems that could collect and process data from various machines in factories or production lines. These "networks" were not using Internet protocols to exchange data. In fact, they usually did not have external connectivity, so security was not a top concern.

Another problem is that people do not generally focus on security when setting up IoT devices (Manifavas et al., 2014). When configuring IoT devices the usual behaviour of the users will be to use the default configuration (ex. default password). Such action must be discouraged as it creates one of the most common vulnerabilities.

Widespread attacks on IoT devices are not a theoretical concept – they have already happened. This is illustrated by the Mirai Malware (Kolias et al.,2017) which was discovered in 2016 which targeted devices such as internet-enabled cameras (IP cameras) and other IoT products and ultimately disrupted the service of many news and media websites. These attacks were successful because the Mirai malware used common default credentials (such as a username and password being set by the manufacturer as 'admin') and poor configuration of devices. These weaknesses are frequently identified in IoT products.

In the case of Mirai, compromised devices were grouped together as a network (known as a botnet), controlled by an attacker and used to launch DDoS attacks against other internet-connected devices and services. The Malware[1] was used in several high-profile attacks, including against the French cloud computing company OVH, and internet services company Dyn – temporarily preventing users worldwide accessing popular platforms such as Netflix, GitHub, and Twitter.

2.2 Healthcare System

In this section we will give a description of the healthcare system infrastructure by giving a short introductory definition of the system and following up with the description of system topology, networking and vulnerabilities.

2.2.1 Description

Recently McAfee, one of the world's leading computer security companies, published a report entitled "80 to 0 in Under 5 Seconds: Falsifying a Medical Patient's Vitals". (McKee, 2018).

The study addresses the problem of Cyber Security in healthcare, a problem that emerges with increasing urgency as digitization advances in this area and must be addressed with appropriate solutions.

Today, Cyber Security is the biggest obstacle and challenge to the efficient evolution of the healthcare sector. It is therefore necessary to provide this sector with appropriate solutions that can restore a climate of trust in digital innovation by ensuring the highest levels of security and privacy for the data of all those involved.

As Artificial Intelligence (A.I.) spreads in the healthcare sector, it is easy to predict that the attacks allowed by the increasing use of A.I. can be particularly effective, finely targeted,

[1] Mirai as a Malware - https://en.wikipedia.org/wiki/Mirai_(malware)

difficult to attribute, and able to exploit the vulnerabilities of A.I. systems used by those responsible for defending systems.

The use of A.I. to automate tasks related to the execution of cyber-attacks will reduce the gap between the scope and effectiveness of attacks. This may expand the threat associated with labor-intensive cyber-attacks (such as spear-phishing or targeted fishing) or new attacks that exploit human vulnerabilities (e.g., through the use of speech synthesis for impersonation), existing software vulnerabilities (e.g., through automatic hacking) or vulnerabilities of A.I. systems themselves (e.g., through adversarial learning or automatic learning in hostile environments and through data poisoning).

AReSS Puglia, the Regional Strategic Health and Social Agency of Puglia is a technical-operational and instrumental body of the Region to support definition and management of social and health policies. Its epidemiological division, *Epidemiology and Care Intelligence*, produces, analyzes and interprets the data about hospitalization, mortality, health and social-health services. Among its many tasks, we can find the management of the informatics *Cancer Registry*.

The *Cancer Registry* was established by D.G.R. (Resolution of the Regional Government) n. 1500/2008, with a Coordination Centre and six peripheral sections in the local health unit which use standardised and homogeneous procedures in line with the reference documents of national and international accreditation bodies (Regione Puglia, 2018).

The databases that feed the Register are several and contain extremely sensitive data:

- register of persons eligible for assistance
- archive of hospital discharge cards
- regional register of causes of death
- informatics archive of the pathological anatomies
- hospital register of medical records
- and organ pathology registers.

In consideration of its enormous amount of sensitive data, some of the common threats are:

- security gaps in database containing sensitive data (data concerning health) systems
- loss of control over computer systems
- and unauthorized access to information systems that would jeopardize the health and personal data of patients as well as the organisation itself.

But weaknesses are about data too:

Data availability, i.e. protection of information assets in the guarantee of access, usability and confidentiality of data. From a security management point of view, it means reducing to acceptable levels the risks connected with access to information (intrusions, data theft, etc.).

Data integrity, intended as a guarantee that the information will not be modified or deleted as a result of errors or voluntary actions, but also as a result of malfunctions or damage to technological systems.

Data confidentiality, i.e. management of security in such a way as to mitigate the risks associated with access to or use of information in an unauthorized manner.

.

2.2.2 System architecture and infrastructure

The above mentioned **Cancer Registry** is led by the team of the Epidemiology and Care Intelligence Area (*Coordination Center of the Cancer Registry of Puglia*). It works in partnership with the cancer registry teams of the local health units of Puglia and performs coordination and support functions for them, as shown in the following diagram.

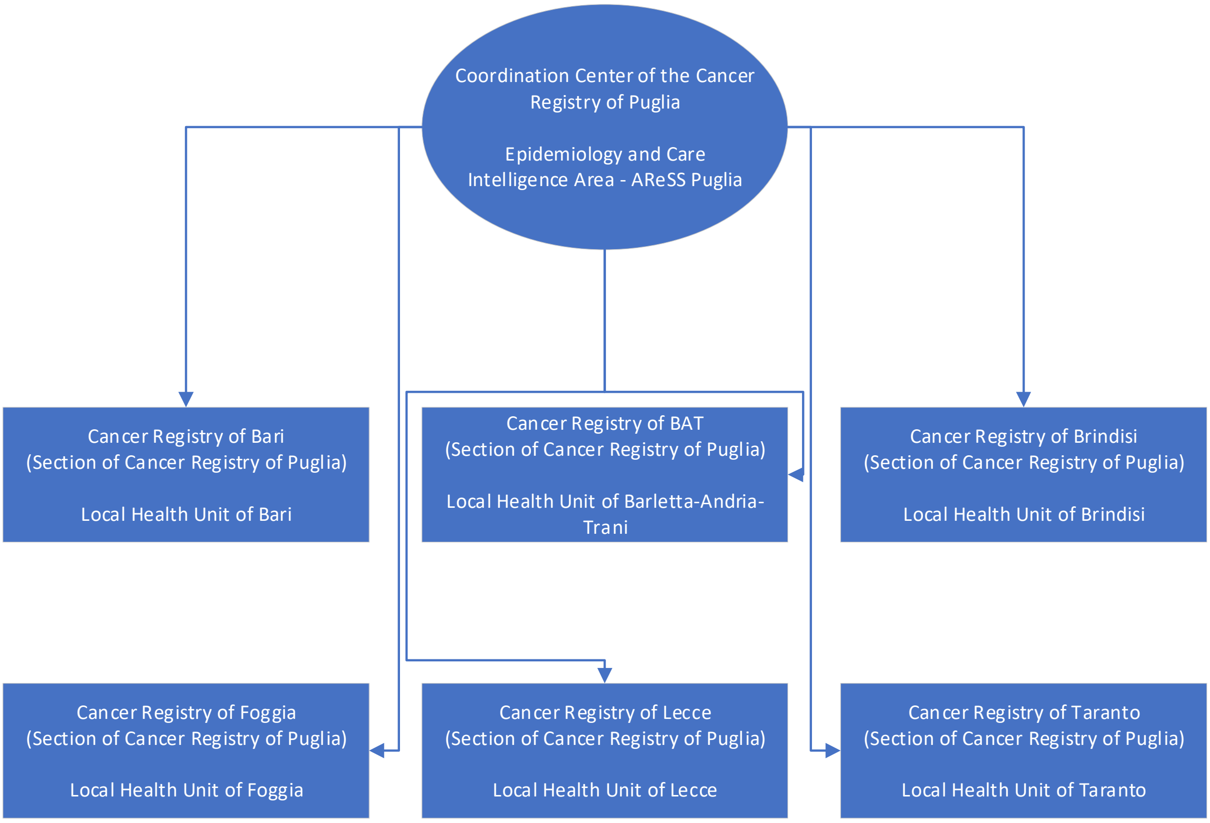

Coordination Center of the Cancer Registry of Puglia
Epidemiology and Care Intelligence Area - AReSS Puglia
Cancer Registry of Bari (Section of Cancer Registry of Puglia)
Local Health Unit of Bari
Cancer Registry of BAT (Section of Cancer Registry of Puglia)
Local Health Unit of Barletta-Andria-Trani
Cancer Registry of Brindisi (Section of Cancer Registry of Puglia)
Local Health Unit of Brindisi
Cancer Registry of Foggia (Section of Cancer Registry of Puglia)
Local Health Unit of Foggia
Cancer Registry of Lecce (Section of Cancer Registry of Puglia)
Local Health Unit of Lecce
Cancer Registry of Taranto (Section of Cancer Registry of Puglia)
Local Health Unit of Taranto

Figure 2. Organisation of Puglia Cancer registry

The information system that allows these teams to work together reflects the structure of the Cancer Registry:

- There is a virtual server at InnovaPuglia – the in-house IT partner of the Region – which hosts the Cancer Registry database. This database contains the cases of cancer of the population living in Puglia and the related personal health data.
- Members of the teams in the Local Health Units use a client desktop application that connects to the database in order to enter data and for consultation purposes.
- The exchange of data between clients and the database server takes place on a secure connection on top of the "RUPAR Puglia" network, a network that connects the IT centers and the devices of the regional public and health institutions of Puglia.

The following diagram illustrates the concepts expressed above:

.

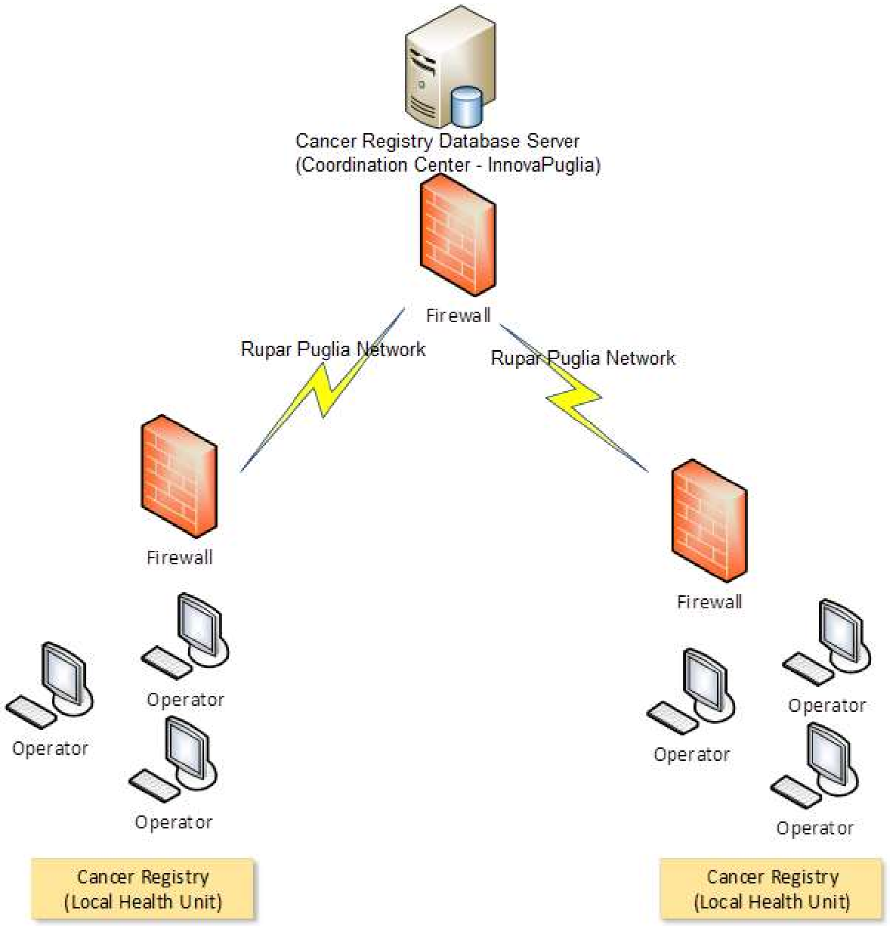


Figure 3: Cancer Registry information system.

- This work model could show several critical issues:
    - The database does not accept connections from clients other than those recognized, but someone could mimic the behavior of a regular client and gain access to the sensitive data.
    - AReSS Puglia does not have access to the PCs/workstations used by the operators of the local cancer registries, because they are property of the respective local health units.
    - The Coordination Centre of the Cancer Registry of Puglia does not know if those PCs/workstations are well protected or if the health data exchanged with the database server are securely processed, so it is very important that Coordination Center and every local health unit is properly trained to manage with Cyber Security threats.
    - Involving Third-party suppliers (Supply Chain Cyber Risk) can determine some critical security issues.

The variety of sources [e.g. EDOTTO (Puglia Regional Information Health System), ISTAT (Italian Institute of Statistic)] through which the database is fed may represent a vulnerability of the system, in consideration of the potential error in data accuracy.

2.3 Shipping Smart Systems

In this last section of pilot systems definition, we will look through the shipping smart system infrastructure. An introduction in system components and vulnerabilities will be followed by a description on system topology, networking and communication protocols.

2.3.1 Description

Security is not an unknown perception in Shipping industry. Protection from sources that put in jeopardy maritime operation is well acknowledged and highly regulated by a respective statutory framework.

The guidelines for preventing deliberate attacks on ships and port facilities is defined in the International Ship and Facility Security Code ISPS adopted by the IMO (International Maritime Organisation) in 2002[2].

In the era of 4th industrial revolution ships are increasingly using systems that rely on digitization, integration, and automation, which calls a different approach in management of security, threats identification and evaluation. Cyber Risk management on-board is gradually coming in the foreground of consideration.

As technology continues to develop, Information Technology (IT) and Operational Technology (OT) on-board ships are being networked together – and more frequently connected to the Internet. Further to the above, the growing use of big data, AI, smart ships and the IoT, increases the amount of information and volume of data propagation, population and migration in between systems. Vessels are exposed to Cyber Attackers and the potential attack surface to Cyber Criminals. This makes the need for robust approaches to Cyber Security important both now and in the future.

Assessment of Vulnerabilities and Cyber Security strategy could be facilitated by internal experts or supported by external experts with knowledge of the maritime industry and its key processes, resulting in a strategy centred around the key risks. Obviously stand-alone systems will be less vulnerable to external Cyber Attacks compared to those attached to uncontrolled networks or directly connecting to the Internet.

Some common cyber vulnerabilities (Bimcoet al., 2017) could be found on-board and listed as following:

- obsolete and unsupported operating systems;
- outdated or missing antivirus software and protection from malware;
- inadequate security configurations and best practices, including ineffective network management and the use of default administrator accounts and passwords, and ineffective network management which is not based on the principle of least privilege;
- shipboard computer networks, which lack boundary protection measures and segmentation of networks;
- safety critical equipment or systems always connected with the shore side;
- inadequate access controls for third parties including contractors and service providers.

[2] http://www.imo.org/en/ourwork/security/guide_to_maritime_security/pages/solas-xi-2%20isps%20code.aspx

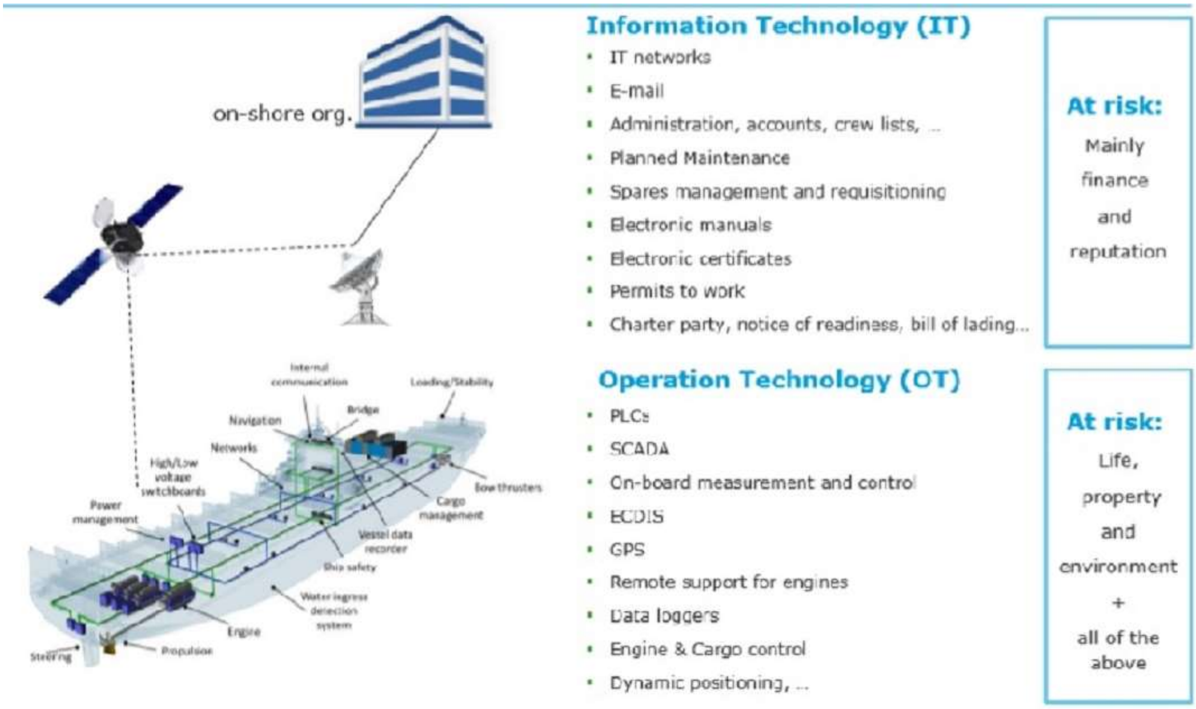
2.3.2 System architecture and infrastructure

The distinction between IT and OT systems should be considered. IT systems focus on the use of data as information whilst OT systems focus on the use of data to control or monitor physical processes.

On-board infrastructure exposed to vulnerabilities includes:

- **Cargo management systems:** Digital systems used for the management and control of cargo, including hazardous cargo, may interface with a variety of systems ashore.
- **Bridge systems**: The increasing use of digital, network navigation systems, with interfaces to shore side networks for update and provision of services, make such systems vulnerable to Cyber Attacks. A Cyber Incident can extend to service denial or manipulation, and therefore may affect all systems associated with navigation, including ECDIS, GNSS, AIS, VDR and Radar/ARPA.
- **Propulsion and machinery management and power control systems:** The use of digital systems to monitor and control on-board machinery, propulsion and steering make such systems vulnerable to Cyber Attacks.
- **Access control systems**: Digital systems used to support access control to ensure physical security and safety of a ship and its cargo, including surveillance, shipboard security alarm, and electronic "personnel-on-board" systems.
- **Crew servicing and management systems & Crew welfare systems**: Digital systems used for property management, boarding and access control may hold valuable crew related data. On-board computer networks used for administration of the ship or the welfare of the crew are particularly vulnerable when they provide Internet access and email.
- **Communication systems:** Availability of Internet connectivity via satellite and/or other wireless communication can increase the vulnerability of ships. The cyber defence mechanisms implemented by the service provider should be carefully considered but should not be solely relied upon to secure every shipboard systems and data

A typical topology of the on-board IT and OT infrastructure (Dnv Gl Maritime Advisory, 2016) which is exposed to Cyber Threats and to risks in the format of environmental, crew safety or financing negative uncertainties is portrayed below.



Information Technology (IT)

- IT networks
- E-mail
- Administration, accounts, crew lists, ...
- Planned Maintenance
- Spares management and requisitioning
- Electronic manuals
- Electronic certificates
- Permits to work
- Charter party, notice of readiness, bill of lading...

At risk: Mainly finance and reputation

Operation Technology (OT)

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

At risk: Life, property and environment + all of the above

Figure 3. Topology of IT and OT infrastructure on-board

Ships are becoming more and more integrated with shore-side operations because digital communication is being used to conduct business, manage operations, and stay in touch with head office. Furthermore, critical ship systems essential to the safety of navigation, power and cargo management have been increasingly digitalised and connected to the Internet to perform a wide variety of legitimate functions (e.g. updates, versioning upgrades, remote maintenance, voyage or ship performance monitoring from ashore, etc.). Ship-shore interface is conducted with several communication methodologies and protocols whistle Cyber Threats could be applicable to the full range of networking.

A schematic approach on the aforementioned networking for consumption of services between two distinct partners (shore and ship, supplier and vessel, third-party OS system provider and vessel, etc.) is following. Figure 4 is displaying and describing the configuration of DANAOS' communication protocols (web services, emails, telco, calls etc.) and security protections. Firewalls applied at each side of junctions between network components and Data protection is secured with not storing data in centralized repositories but with controlling from a tailor-made and internally developed service platform (DANAOSone platform).

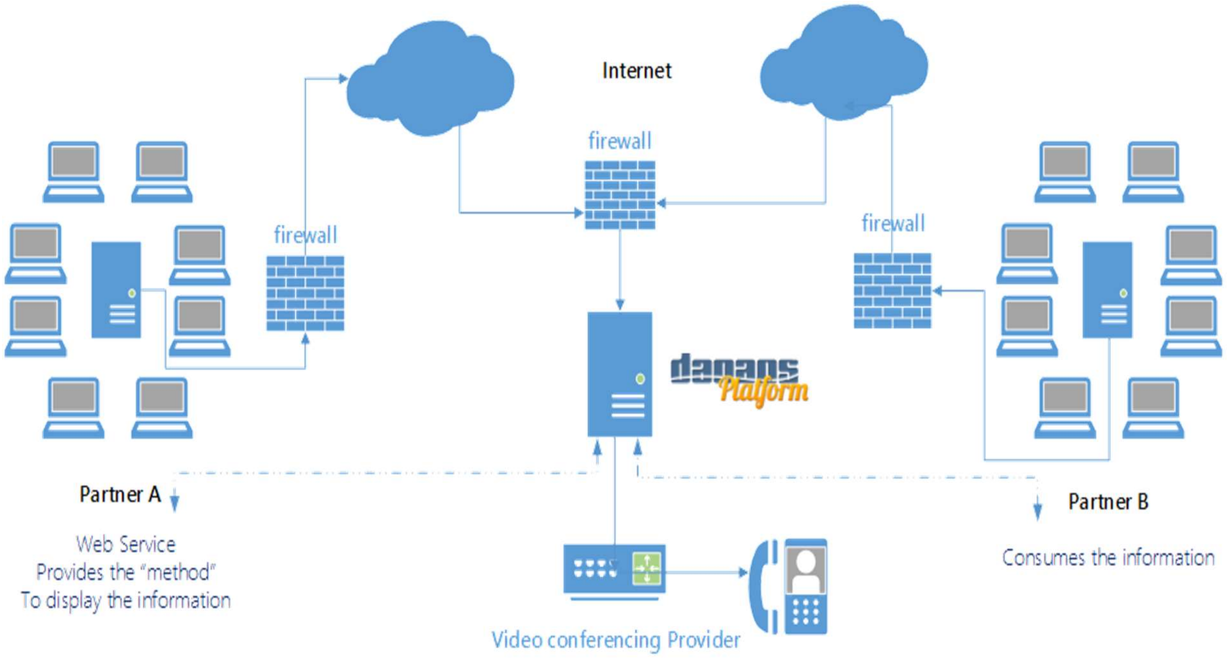


Figure 4. DANAOS configuration of communication protocols

3 Pilot Security Framework and Requirements

3.1 Smart Energy System

3.1.1 Existing Methodologies and Procedures (Best Practices)

Following the most famous IoT protocols their procedure logic is described.

As we mentioned previously MQTT[3] is one of the most frequent used protocols for communication between smart devices. MQTT is an ISO standard and it stands for Message Queuing Telemetry Transport and the first version was issued in 1999. Its main use was for industrial automation and more specifically for transporting short telemetry data messages. For transportation of the data any format can be used as there is no standard defined, hence it is able to virtually carry any payload. The protocol uses the publish-subscribe-based messaging model. It works like an RSS feed: the user subscribes to a topic, and once someone publishes something on the topic, the payload is transported to all subscribers.

As mentioned earlier, on MQTT protocol, including the most common server software that implements this protocol (or broker as it is known in the case of MQTT), which is called Mosquitto, when proper configuration is applied, the currently known security issues are reduced to the minimum. In fact, both MQTT and Mosquitto have broad security capabilities — for example, to provide fine-grained access control by user and topic. As with many things, the problems are created in the implementation and configuration. In the following, some real world use cases for MQTT are described.

MQTT is regularly used, to overcome the gap between different protocols, so that different devices can communicate with each other even if a different protocol is used for the communication. It is very convenient as it allows topics to be ordered in a hierarchical structure, creating a unified namespace for the whole smart environment. For example, a topic structure can look like this:

```
/myhouse/garage/lights/frontlight
/myhouse/garage/lights/ceilinglight
/myhouse/garage/garagedoor
/myhouse/livingroom/tv
/myhouse/bathroom/washingmachine
/myhouse/bathroom/lights
```

The structure is hierarchical, outlining a structure for connected devices in a home. One of the things that makes MQTT useful in smart environment is that it is possible to use wildcards when subscribing to the topics, similar to how filename or search wildcards work. In particular, MQTT has two wildcards: # and *?*

# stands for all levels from its location/occurrence, down the hierarchy, so for example by subscribing to:

```
/myhouse/garage/#
```

[3] MQTT - http://mqtt.org/faq

An IoT device will get any message published to `/myhouse/garage/frontlight` or `/myhouse/garage/ceilinglight` .

The ? stands for all categories on any level and can be used anywhere in the hierarchy, more than once. Hence, by subscribing to:

```
/myhouse/?/lights/#
```

the device will receive all messages regarding the lights in any room, as *?* in this case can be a bathroom or garage, for example.

By combining subscriptions, is it possible to create a very complex scenario for controlling a group of devices by publishing on just one topic. Publishers can be, for example, MQTT-capable light switches. By pressing them, an MQTT message is published and action is taken. Any device can be a publisher, subscriber, or both.

However, to make an actual smart home, automation should be added in the whole system. In fact, home automation usually comes in the form of software, or perhaps a smart box, which contains "business logic" and acts as a "smart home hub" to combine the control of the devices, which is where MQTT acts. MQTT is included in most smart home hub software solutions, such as Home Assistant, so users can either install a package that includes MQTT or install MQTT separately when setting up their smart home hub. Smart home hubs typically subscribe and publish MQTT messages and provide logic.

For example, if the hub gets the message from a motion sensor in the back of a house that some movement was detected and knows that its sundown, it can activate a light or communicate with the alarm system in order for it to trigger. In this way, several smart devices can be connected to a smart hub, controlled, and even automated, using the MQTT protocol, even if they weren't originally designed to work together.

More specifically MQTT process is implemented as:

An MQTT server (broker) sits on the top, with embedded security capabilities, which serves as a "messenger" between all components. A smart home hub orchestrates all of the devices and adds real intelligence to the whole system, as there are various MQTT-capable or MQTT-bridged devices that are connected to the MQTT server/broker.

When the MQTT server does not have a secure configuration, a lot of vulnerabilities appear, resulting to the main issues being insecure and leaving the default configurations on. What makes the misconfiguration of MQTT worse is that by getting access to the MQTT server, everything can be accessed, such as the messages flowing through it using the wildcards mentioned before ("# "and "?"). By using the wildcards anyone can subscribe, for example by using # and receive any publication of any topic. Because subscription happened on the top of the hierarchical chain, any data bellow that chain will be transmitted.

More concerning is that many poorly configured MQTT servers are also publicly available on the internet without any password, allowing a cybercriminal to spy on any house that uses it. The "advantage" for the cybercriminal is that if the server is publicly available, a connection can be made to it from anywhere. Further, as most users don't set up access controls— in the form of Access Control Lists (ACLs)—when they configure a Mosquitto while setting up their smart home hub, cybercriminals can not only subscribe to the server, but can also publish to it, thus seizing control of all devices in a smart home. The vulnerabilities reflected by the total results above are most likely due to misconfigured MQTT servers. As users set up these systems to remotely control their smart home, they often expose not only the "dashboard" or control panel of the system, but also the MQTT server, as these two components usually run on the same machine or server. When this happens, it can leave users exposed. It was found that generally, it is not overly clear to users how they securely configure their MQTT connection during the installation process.

3.1.2 Threat Assessment

In the following, few examples of what can happen in the event the system is misconfigured are described.

a) Connecting and subscribing to wildcard topics on an unprotected MQTT server

Cybercriminals can find an open and unprotected MQTT server and subscribe to the # topic. This is easy enough and, once connected, the attacker will receive every message published. In the case of some home automation systems, the status of window sensors and open/closed doors, as well as every press of any light switch in the house and even the local weather forecast can be reported.

There are usually no ACLs (Access Control Lists), which is a fine-grained access control to the topics in place, so once an attacker is connected, he can also publish to topics. In this case, he can control devices or at least poison the data being collected by publishing on behalf of the devices. For example, he can send messages to the hub as if he was the security sensor at the smart home's front door smart lock, because MQTT messages do not have a sender field so the message receiver is unable to determine where the request came from. Due to this, cybercriminals can easily perform "replay attacks" and send messages on behalf of the devices connected to the hub.

b) Connecting to unprotected smart hub dashboards on a secure MQTT server

A smart home can be hacked even on a secure MQTT server, as sometimes a dashboard (smart home control panel) runs on the same IP address as the MQTT server.

Many homeowners use open source solutions for their smart home. The most popular software for smart hubs is readily available solutions such as Domoticz, Home Assistant and OpenHAB[4]. Examining these systems, a lot of default configurations have been found which surprisingly require no password. So, even if the MQTT server is secure, the dashboard can be accessed as easily as typing the IP address into a browser. By doing this, an attacker can get complete access to the house.

Exploiting this access would allow a cybercriminal to control any of the devices connected via the dashboard including lights, locks, heating and cooling systems, cameras, and more. With this control, a cybercriminal could do any number of things, such as secretly spy on or record people within their home, drastically adjust their home's temperature, or gain entrance to the home while the homeowners are on vacation or at work, without setting off any alarms.

c) Reading files on a protected MQTT server with a protected dashboard

In order to prevent security issues where both the server and the dashboard has been protected, it must also be noted that other services must be checked for exposing security risks.

In the case of the Home Assistant software "smart hub," several instances of properly configured MQTT servers have been found that were not exposed and their dashboard that was

[4] Domoticz vs Home Assistant vs OpenHAB- **https://www.smarthomeblog.net/openhab-home-assistant-domoticz/**

properly configured and password-protected. Those servers though had open and unsecure SMB shares.

SMB is a protocol used for sharing files on internal networks, mainly on the Windows platform. It was found that publicly shared directories were exposed with all the Home Assistant files including configuration files.

It is believed that the problem arises when the users are not aware of the fact that once they install HomeAssistant on the server (in this case it's probably HASSBIAN flavour of HomeAssistant intended as a readymade package for installation on various types of underlying hardware) and expose it to the internet to get access into the dashboard, they also often expose a Samba share that is used for accessing the configuration and installation files of HomeAssistant. By doing this, they unwillingly leave the whole system exposed to anyone and leak all the passwords and API keys stored there to the public. It has to be noted that even the tech savvy users sometimes lack basic knowledge of how to properly secure their open source systems.

d) Creating a User Interface on an unprotected MQTT server

There are some interesting tools/apps out there that let you create a simple dashboard for an MQTT-based smart home. With the help of an application called MQTT Dash for Android and iOS, a dashboard and a control panel can be created for each home by placing various tiles on the screen and linking them with MQTT topics. An interesting feature of the application is that it can store the layout of the dashboard and the configuration. Instead of creating a special file on each device, settings can be published to the topic of the MQTT server, and by doing so, it can easily replicate these settings on as many devices as requested.

That's very convenient, but if the MQTT server is not secured properly, a cybercriminal can easily get the same UI (User Interface) as the user. This provides an easy way to hack someone's home and even get their UI with just one connection to their MQTT server. Again, the default configuration makes it easier, and if there is a dashboard in use, such as one set up with the MQTT Dash app, one will most likely find a topic with the name "metrics/exchange," a so-called "retained" topic. If a subscription is made to a retained topic, then the subscriber can receive the last stored payload/data, which basically means the whole dashboard will be loaded easily.

e) Tracking device location

MQTT servers typically concentrate on a lot of interesting and real time data. Many MQTT servers have been found, which were not even connected to a smart home system, containing one very interesting topic beginning with owntracks. By doing a simple Google search, anyone can find and install OwnTracks which is an Android and iOS application that works as a personal GPS tracker. An interesting thing about the application is that it supports the MQTT protocol while it can also share your location with your friends or family. This would sound reasonable nowadays but the feature needs to usually be configured by connecting to an MQTT server without any encryption or authorization. Moreover, to be able to connect any phone to an MQTT server, it will be first exposed to the internet. Unfortunately, many users setup the configuration without considering any security measures. OwnTracks then sends a JSON message to the MQTT topic `owntracks/`… each time a phone device changes location.

That JSON message contains unique and important information of the user such as:

- lon (longitude), lat (latitude) and alt (altitude).

- battery level of the phone.
- timestamp for the position of the user, named as “tst” in the UNIX epoch format. After decoding it to a more ‘readable’ format, it can be then be read as a simple timestamp (ex. Tue 7 August 2018 11:26:48 UTC).

By using all this information someone’s position during the day, month or year can be easily reconstructed.

So, while this is a huge issue, because that information is available as real-time data, many users will simply share their location for the reason of providing automation and convenience. Some of the “smart home” hubs or systems request users to share their position with the excuse of providing them with a better experience. Some real world scenarios where that better experience is applicable, is when your house automatically turns on the lights as you get close to home, or, when the system is configured to turn off all the lights whenever nobody is at home.

The sharing of GPS location information is exactly what the system needs to provide this functionality. The problem here again is security, more specifically, unsecured protocols and unencrypted OwnTracks messages. Main reason behind that is because users usually rely on default configurations.

To conclude:

Because there are still many poorly secured protocols dating back to bygone technology eras when security was not a top concern, it is frighteningly easy to gain access and control of a person’s smart home. The convenience of IoT devices and smart home hubs connected to the internet is a double-edged sword, and there is a trade-off between ease-of-use and security.

Consumers need to be aware of the security concerns of connecting devices that control personal parts of their home to services they don’t fully understand and the importance of properly configuring their devices. Industry-wide, better device-level security has been requested for IoT devices. In order to ensure users’ entire smart home ecosystem is secured, manufacturers need to develop IoT devices which are simple for consumers to set up with a high-level of security. Lastly, there is a need for more secure control solutions that allow consumers to confidently use technology in their homes with the knowledge that it is secure and their privacy protected

3.1.3 Training requirements

Business processes can transform by using the Internet of Things (IoT) over connectivity, analysis and automation. While new IoT systems are introduced, developed and integrated into company communication networks, new attacks arise along with them, that expose those systems. These attack areas provide competitors with new ways to steal services, compromise information or activate worst-case physical scenarios against connected infrastructures. The target groups which consist of security practitioners and information technology staff must be able to methodically analyze threats to IoT devices, information, and the infrastructure that supports them in order to select the correct security solutions and procedures for securing an IoT-enabled business.

The IoT is broad in scope and incorporates all industries in numerous forms. Many IoT devices exist each its specific purpose such as, connecting electric vehicles and smart grids at the larger end of the scale, to single-purpose sensors comprised of a microcontroller, sensor, battery and not much more. Soon, IoT devices of different type will increase exponentially on the Distributed Energy sector, in which the Organizations using them will have to implement additional safety and security measures, due to their ability to cause effects in the physical world. These Organizations called by Cyber Physical Systems (CPS) will be the main attack targets and the appropriate concern should be afforded to them in an Enterprise IoT Security Program.

The core goal is, information technology professionals to be trained and security engineers to be responsible for architecting and implementing new IoT-based solutions within the customers' base.

It is expected that, the Thread Arrest training platform will provide the steps required for designing and implementing an IoT Security Program.

Unique threats associated with the IoT must be identified and compared with the differences when related with traditional Information Technology (IT) systems. A guide can be created that will cover the employment of an IoT security lifecycle within our clients that includes robust security engineering procedures, the ability to integrate IoT devices into existing security infrastructures, and the detailed information regarding how to achieve an IoT Privacy Impact Assessment (PIA) and Safety Impact Assessment. Lastly, the platform is also expected to discuss how will a secure IoT device will be created and how will that later integrate with other IoT devices securely to the Cloud.

3.2 Healthcare Cyber Security Training

3.2.1 Existing Methodologies and procedures (best Practices)

With the increase in networked objects in the hospital environment, the healthcare sector is also increasingly becoming a victim of Cyber Crime.

For this reason, the European Union Agency for Network and Information Security (ENISA) published on 24 November 2016 “Smart hospitals - Security and resilience for smart health service and infrastructures” (ENISA, 2016), which proposes some key recommendations for information security in the world of health, particularly in hospitals.

The research, carried out with the support of experts from different sectors, focuses first on documents and empirical data, and then analyze potential attack scenarios, such as attacks on hospital staff through social engineering techniques, tampering or theft of equipment or medical devices, ransomware attacks and DDoS attacks.

The document also proposes some 'recommendations' and best practices, both organizational and technical. These include precisely indicating roles and responsibilities for security; creating Cyber Security policies and procedures; developing training and awareness programs; identifying risks, resources and threats; drawing up contingency plans; adopting high standards; conducting consistent security audits; and using contractual clauses with suppliers; implement intrusion control; increase the use of firewall equipment; use anti-malware software; make regular data backups; best configure and manage resources; use update procedures; strengthen user access control; enforce the use of encryption; and classify data and protect remote and mobile health systems.

Looking at the U.S. system, in the Cyber Security Act of 2015 (the Act), Congress established the Healthcare Industry Cyber Security (HCIC) Task Force to address the challenges that the Healthcare industry faces when securing and protecting itself against Cyber Security incidents, whether intentional or unintentional.

On June 2017, Healthcare Industry Cyber Security Task Force released a "*Report on improving Cyber Security in the Healthcare industry*" indicating some "imperatives" (Healthcare Industry Cyber Security Task Force, 2017):

1. Define and streamline leadership, governance, and expectations for Healthcare industry Cyber Security.
2. Increase the security and resilience of medical devices and health IT.
3. Develop the Healthcare workforce capacity necessary to prioritize and ensure Cyber Security awareness and technical capabilities.
4. Increase Healthcare industry readiness through improved Cyber Security awareness and education.
5. Identify mechanisms to protect research and development efforts and intellectual property from attacks or exposure.
6. Improve information sharing of industry threats, weaknesses, and mitigations.

In February 2014, N.I.S.T. (U.S. National Institute of Standards and Technology) released the Framework for Improving Critical Infrastructure Cyber Security (Cyber Security Framework) as directed in Executive Order 13636, Improving Critical Infrastructure Cyber Security (National Institute of Standards and Technology, 2018).

The Cyber Security Framework provides a voluntary, risk-based approach - based on existing standards, guidelines, and practices – to help organizations in any industry to understand, communicate, and manage Cyber Security risks.

In the Healthcare space, entities regulated by the Health Insurance Portability and Accountability Act (HIPAA) must comply with the HIPAA Security Rule to ensure the confidentiality, integrity, and availability of electronic Protected Health Information (ePHI) that they create, receive, maintain, or transmit (U.S. Government, 1996).

3.2.2 Threat Assessment

Healthcare Sector experienced more cyber incidents resulting in data breaches than any of the other 15 critical infrastructure sectors. These incidents underscore the concerns about organizations having neither the awareness of current threats nor the technical personnel to prevent or deal with these threats, many of which are not new.

The increased focus on Cyber Security provides an opportunity for the Healthcare industry to adapt and improve Cyber Security through awareness rising and training. The type of threat actors that can become potential attackers and the attack vectors they can affect should be known by defenders. Threat actors in Healthcare organizations include:

- Insider threats: (physicians, nurses, or even administrative staff that has a malicious intent to harm the ICT systems).
- Malicious patients and guests.
- Remote attackers: remote care provision and the use of this equipment for malicious actions could be a possible scenario when the attacker is not physically in the hospital.
- Other causes: Environmental or accidental equipment/software failure or even external maintenance staff can cause security incidents, yet have no active attacker.

Regarding attack vectors in local health units, we can find:

- Physical interaction with IT assets (patients or physicians).
- Wireless communication with IT assets: attacking within range of wireless technologies, is the most common.
- Wired communication with IT assets: Attackers with wired network communications (including access to the Internet) can interact with related IT assets including cloud services, and online healthcare information systems.
- Interaction with staff: Social engineering attacks are very common in the healthcare sector, it is usually where ransomware starts from.

Potential attack points and threat types are based on the key assets and a series of root causes. The root causes of threats faced by Health organizations are **malicious actions, human errors, system and third-party failures and natural phenomena**.

1. **Malicious actions** are deliberate acts by a person or an organisation. Although both threaten Health organisations, it is important to distinguish malicious actions from other deliberate actions that bypass policies and procedures without malicious intent. The goals of attackers are performed using:

- Malware: worms (which spread between computers), trojans (which act covertly), viruses (which spread internally), rootkits (which hide infection), exploitkits (which exploit vulnerabilities in clients to infect systems), botnets (which place many infected systems under control), spyware (which monitor systems)
- Hijacking
- Social engineering attacks (e.g. phishing, baiting)
- Device and data theft are also relevant in the context of malicious attacks
- DoS/DDoS attacks might render a system or service altogether unavailable, which could potentially fully disrupt a patient care process, just as shown in the figure
- Combinations of all the abovementioned methods

.

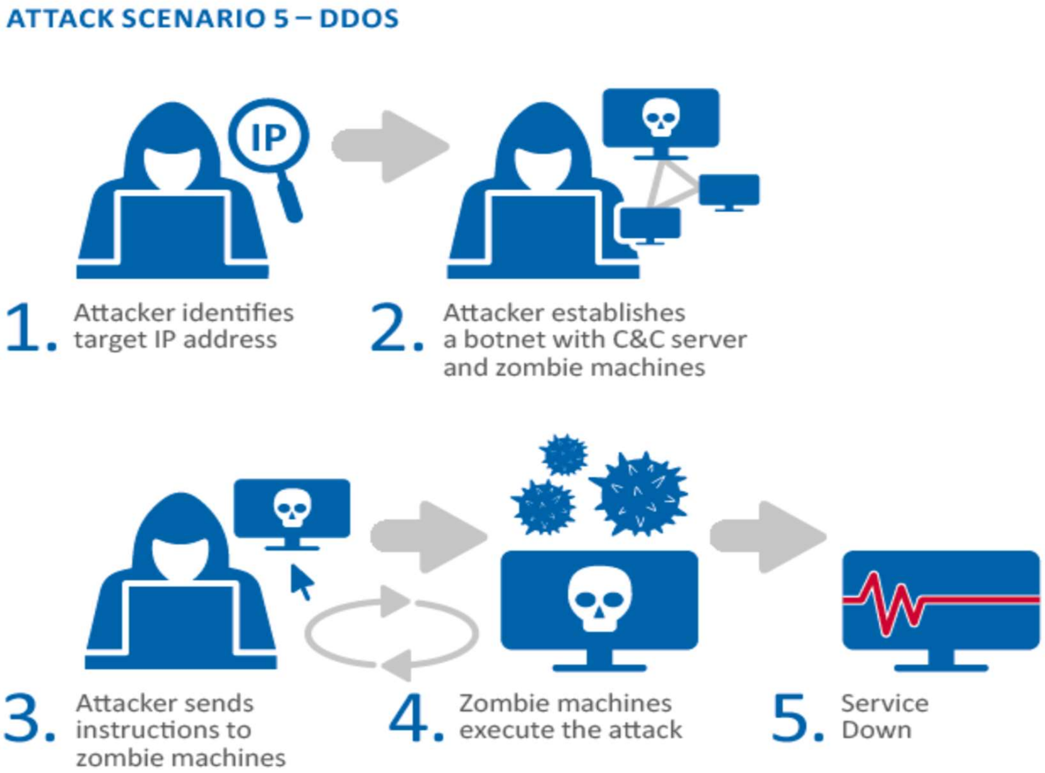

ATTACK SCENARIO 5 – DDOS
IP
1. Attacker identifies target IP address
2. Attacker establishes a botnet with C&C server and zombie machines
3. Attacker sends instructions to zombie machines
4. Zombie machines execute the attack
5. Service Down

Figure 5. DDOS Attack Scenario.

2. Human errors occur during the configuration or operation of devices or information systems, or the execution of processes. Human errors are often related to inadequate processes or insufficient training. These include:

- System configuration error that may compromise either the operation or the Cyber Security posture of the system, or both.
- Absence of audit logs to allow for appropriate control – e.g. of access to smart hospital resources – and/or incident identification and assessment of corrective/improvement actions.
- Unauthorized access control or lack of processes is highly pertinent to smart hospitals particularly due to the sensitivity of patient data involved and due to the fact that the medical processes involve roles with a high level of specialization in different domains.
- Physician and/or patient errors are a major threat in the context of a health organization where there is heavy reliance on ICT assets but the users are not experts (e.g. Medical staff).

3. System failures are highly relevant in the healthcare context, particularly due to the increasing complexity and dynamics of the systems. Examples include:

- Software failures that impact or completely disrupt a medical (e.g. failure of a PACS) or administrative process (e.g. patient data availability compromised).
- Network components failure can cause great impact as the interconnected nature of IoT systems and the need for resilient networking is a core requirement for the functioning of a local health unit.

- Insufficient maintenance which may leave operational issues undetected and unresolved, both in terms of Cyber Security posture, but also in terms of patient care operations.
- Overload can lead to unavailability of a system or service.

4. Supply chain failure is outside the direct control of the affected organization as it typically affects or falls under the responsibility of a Third-party. As Healthcare organizations are increasingly dependent on third parties, third-party failures may have far-reaching consequences for them. Examples of third parties a failure of which would have an adverse impact on the operations of the Register include:

- Hosting service providers for medical data, applications, systems, administrative data, and remote patient data collection points.
- Network providers, such as Internet Service Providers (ISPs), that support wide area network connectivity and, thus, access to remote data, systems hosted outside the health local unit's data center including regional systems.
- Power suppliers, a high cross sector dependency that can be partially mitigated.

Even if **Natural phenomena** are not cyber threats, they may also be the cause of incidents, particularly due to their disruptive or destructive impact (earthquakes, flood, fires, etc.).

3.2.3 Training requirements

The effectiveness of a Healthcare organisation's processes directly correlates with how consistent staff are in following those processes. To that end, organisations should provide comprehensive training on Cyber Security measures and the risks involved if staff members are not diligent about these efforts.

They should also be instructed to reach out to IT staff if there is any doubt about an email's authenticity. Both orientation and refresher training should be offered to ensure that the employees are regularly updated about new threats and security measures.

Regular trainings and awareness raising seem to be considered not particularly effective or not yet widely implemented in Health organisations. Healthcare organisations must develop a strategy for Cyber Security hygiene for existing and legacy equipment, a systematic approach for patching, implementation of compensating controls, isolation, and/or replacement (as available or applicable) should be applied.

The following lines describe the established processes within the "Pilot" as will be implemented:

1. **Identify**. Through various procedures and in-depth analysis, Secure Knowledge Management team members identify the organisation's knowledge of Cyber Security. Our key strategy is to enable and empower management to identify and address risk to organisational assets, people, information, software, hardware, telecommunications and facilities.
2. **Protect**. To protect the identified risks: Access Control – Awareness Training – Data Security – Information Protection Processes and Procedures – Maintenance – Protective Technology.
3. **Detect**. Detect and monitor security events implementing effective tools that will actively monitor the organisation's operations and services to identify events before

they develop into a security incident: Anomalies and events – Security Continuous Monitoring – Detection Processes.

4. **Respond.** Secure Knowledge Management staff will plan, test and operationalize any Cyber Security events and incident management processes. We also train security teams to be aware of Cyber Security Threats and we will test the organisation's response to events and incidents. Key processes include: Response Planning – Communications – Analysis – Mitigation – Improvements.
5. **Recover.** The organisation will quickly return to full operational capacity after an attack.

The following picture describes the overall process:

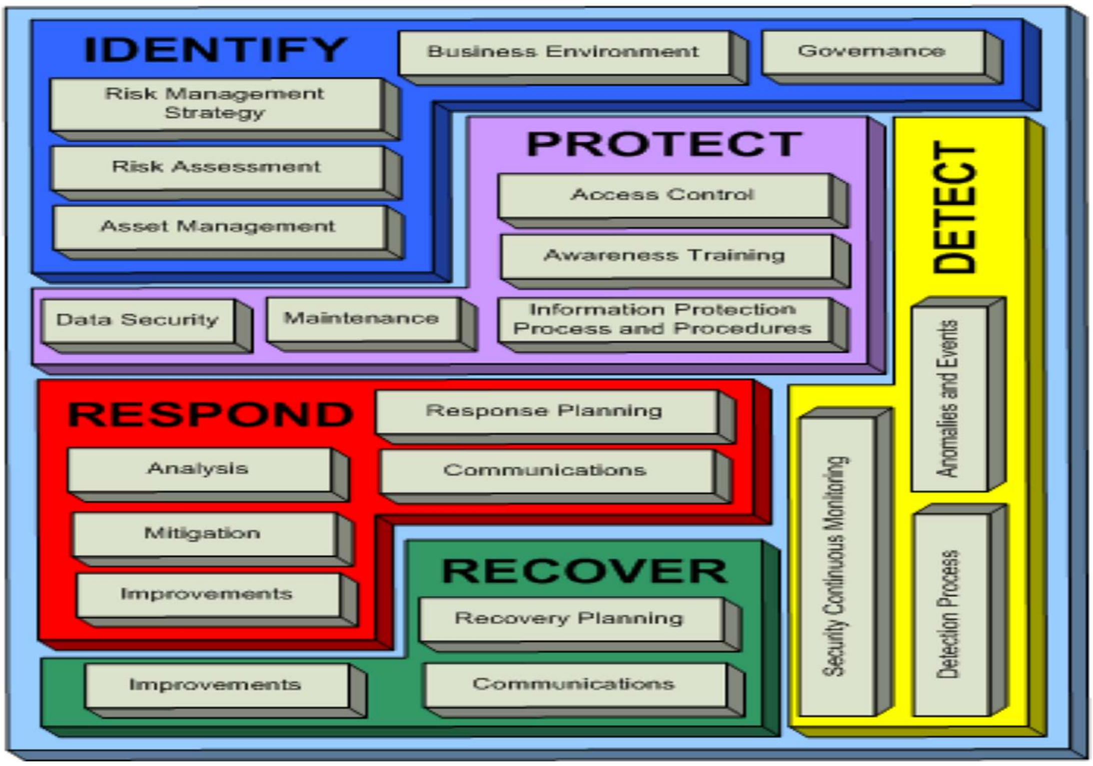


Figure 6. NIST Cyber Security framework

For the Registry, the implementation can be represented in the following picture:

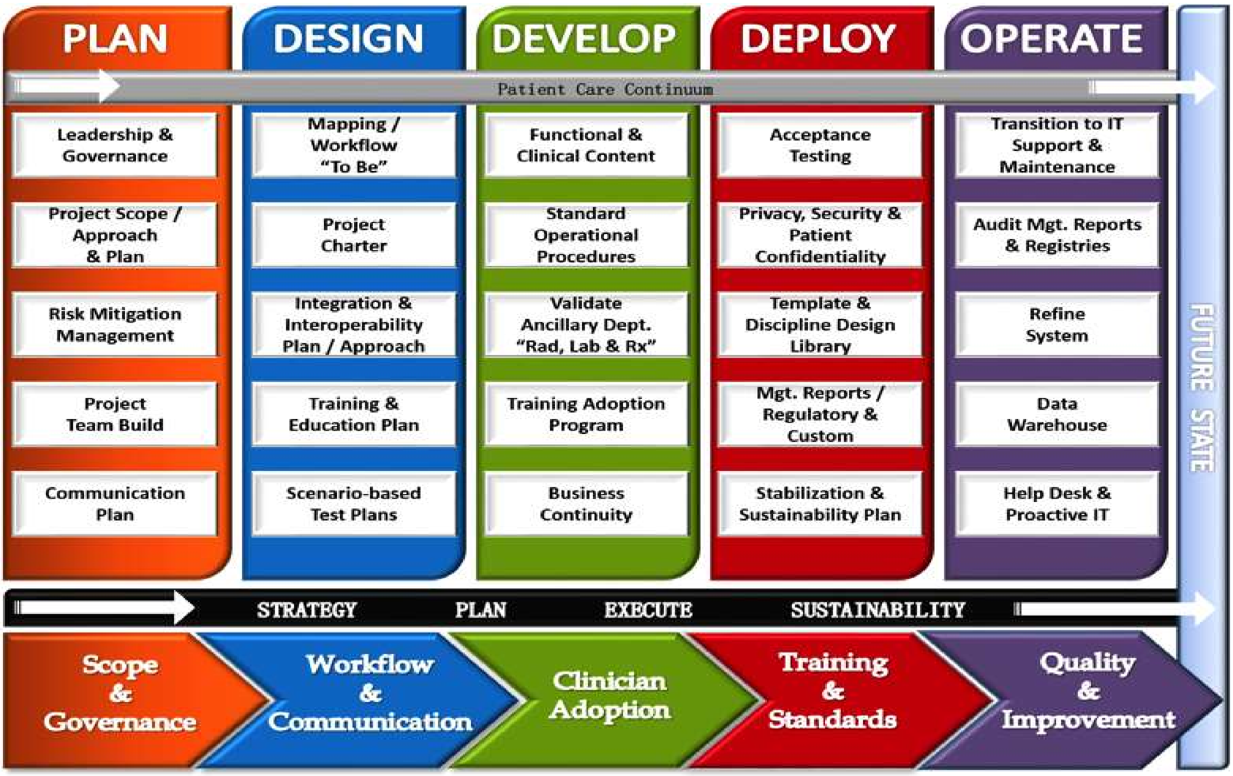

PLAN
DESIGN
DEVELOP
DEPLOY
OPERATE
Patient Care Continuum
Leadership & Governance
Project Scope / Approach & Plan
Risk Mitigation Management
Project Team Build
Communication Plan
Mapping / Workflow "To Be"
Project Charter
Integration & Interoperability Plan / Approach
Training & Education Plan
Scenario-based Test Plans
Functional & Clinical Content
Standard Operational Procedures
Validate Ancillary Dept. "Rad, Lab & Rx"
Training Adoption Program
Business Continuity
Acceptance Testing
Privacy, Security & Patient Confidentiality
Template & Discipline Design Library
Mgt. Reports / Regulatory & Custom
Stabilization & Sustainability Plan
Transition to IT Support & Maintenance
Audit Mgt. Reports & Registries
Refine System
Data Warehouse
Help Desk & Proactive IT
FUTURE STATE
STRATEGY
PLAN
EXECUTE
SUSTAINABILITY
Scope & Governance
Workflow & Communication
Clinician Adoption
Training & Standards
Quality & Improvement

Figure 7. NIST Cyber Security operations

The Healthcare Cyber Security Training scenario will provide reusable threat models and a clear assignment of responsibility for handling them, identifying personnel to be trained. An educated workforce is crucial for healthcare organisations entrusted with strategic public health data and sensitive patient data.

3.3 Shipping Smart Systems

3.3.1 Existing Methodologies and procedures (best Practices)

Cyber Security is not only an application of IT tools to build up a robust system against potential vulnerabilities and protect OT and IT from attacks and threats (Bimco et al., 2017). It considers a holistic strategic framework consisting of three main pillars namely processes (see figure 8), technology and people associated and engaged in Cyber Risk management (Dnv Gl Maritime Advisory, 2016).

Cyber Risk management should:

- identify the roles and responsibilities of users, key personnel, and management both ashore and on-board
- identify the systems, assets, data and capabilities, which if disrupted, could pose risks to the ship's operations and safety
- implement technical measures to protect against a Cyber Incident and ensure continuity of operations. This may include configuration of networks, access control to networks and systems, communication and boundary defence and the use of protection and detection software
- implement activities and plans (procedural protection measures) to provide resilience against Cyber Incidents. This may include training and awareness,

software maintenance, remote and local access, access privileges, use of removable media and equipment disposal

- implement activities to prepare for and respond to Cyber Incidents

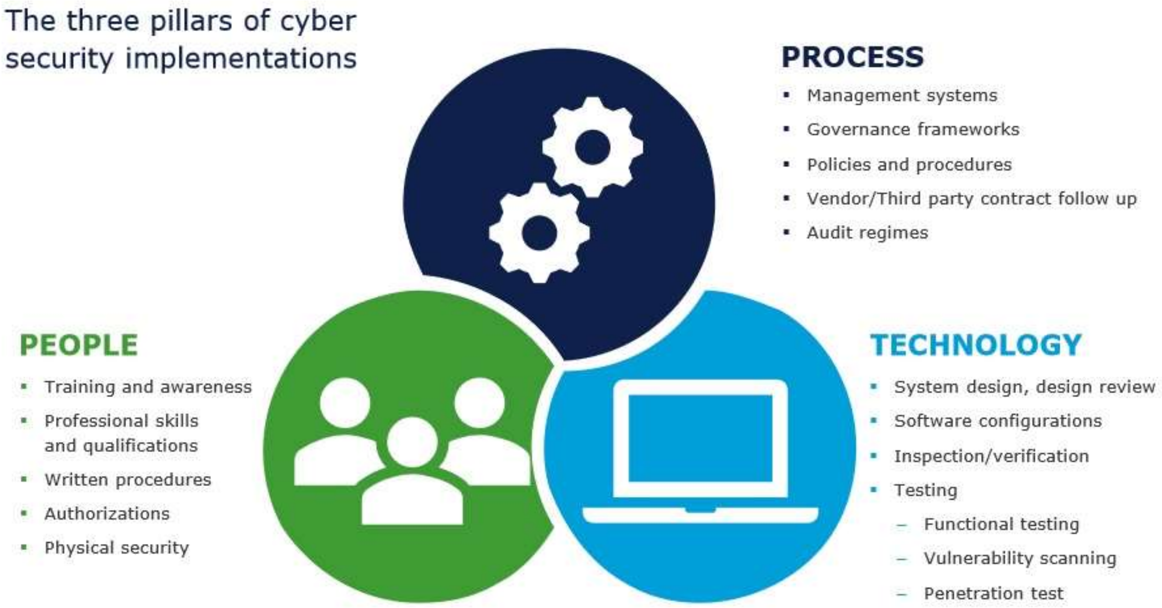


Figure 8. The Three Pillars of Cyber Security management

Risk assessment and Cyber Security strategy is targeting at reduction of exposure to threats and set-up of contingency plans and mitigation actions. A secure network depends on the IT/OT set up on-board the ship, and the effectiveness of the company policy based on the outcome of the risk assessment

Special attention should be given when there has been no control over who has access to the on-board systems. This could, for example, happen during drydocking, layups or when taking over a new or existing ship.

Cyber Security protection measures may be technical and focused on ensuring that on-board systems are designed and configured to be resilient to Cyber Attacks. Protection measures may also be procedural and should be covered by company policies, safety management procedures, security procedures and access controls.

Implementation of Cyber Security controls should be prioritized, focusing first on those measures, or combinations of measures, which offer the greatest benefit.

DANAOS is following the guidelines of the Center of Internet security (CIS) [5]to apply critical security controls to equipment and data on-board vessels

High level of technical protection measures (Bimco et al., 2017) are extended but not limited to several factors, as they are detailed below.

Limitation to and control of network ports, protocols and services
Only appropriate traffic is allowed via a controlled network or subnet, based on the control policy of that network or subnet.

[5] https://www.cisecurity.org/

Configuration of network devices such as firewalls, routers and switches

Controlled networks are designed to prevent any security risks from connected devices by use of firewalls, security gateways, routers and switches. Uncontrolled networks may pose risks due to lack of data traffic control and they are isolated from controlled networks, as direct Internet connection makes them highly prone to infiltration by malware.

On-board networks should normally accommodate the following:

1. necessary communication between OT equipment
2. configuration and monitoring of the OT equipment
3. on-board administrative and business tasks including email and sharing business related files or folders,
4. recreational Internet access for crew and/or passengers.

Effective network segmentation is a key aspect of “defence in depth”. OT, IT and public networks should be separated or segmented by appropriate protection measures. The protection measures used include, but are not limited to an appropriate combination of the following:

- a perimeter firewall between the on-board network and the Internet
- network switches between each network segment
- internal firewalls between each network segment
- Virtual Local Area Networks (VLAN) to host separate segments.

Network segmentation is portrayed in the following picture

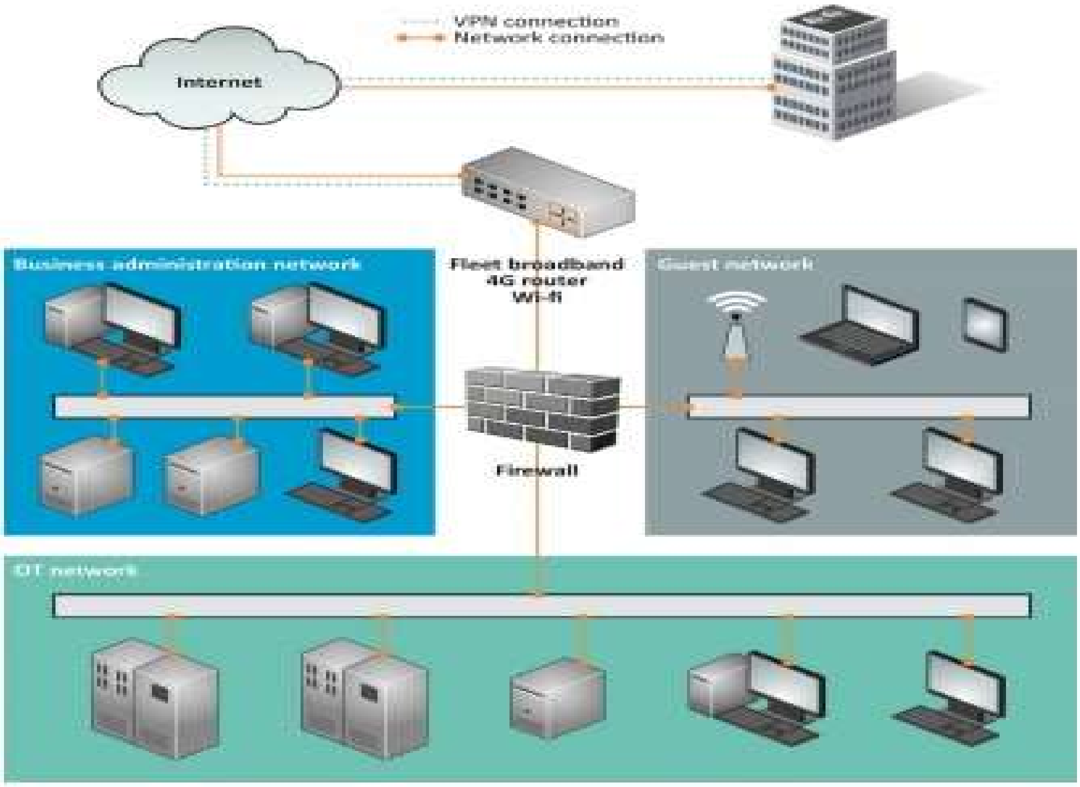


Figure 9. Network segmentation schematic

Physical security
Security and safety critical equipment and cable runs are protected from unauthorized access

Detection, blocking and alerts
Identifying intrusions and infections is a vital part of the controls. DANAOS chooses to incorporate an Intrusion Detection System (IDS) or an Intrusion Prevention System (IPS) into the network or as part of the firewall. Some of their main functions include identifying threats/malicious activity and code, and then logging, reporting and attempting to block the activity

Satellite and radio communication
Cyber Security of the radio and satellite connection is considered in collaboration with the service provider. The access interconnect is the distribution partner’s responsibility. The final routing of user traffic from the Internet access point to its ultimate destination on-board (“last mile”) is the responsibility of DANAOS. When using a Virtual Private Network (VPN), the data traffic is encrypted to an acceptable international standard. Furthermore, a firewall in front of the servers and computers connected to the networks (ashore or on-board) are deployed. Satellite communication terminals and other communication equipment have provided management interfaces with security control software that are accessible over the network.

Wireless access control
Wireless access to networks on the ship is limited to appropriate authorized devices and secured using a strong encryption key.

Malware detection
Scanning software that can automatically detect and address the presence of malware in systems on-board is regularly updated. Anti-virus and anti-malware software is installed, maintained and updated on all personal work-related computers on-board.

Secure configuration for hardware and software
Only senior officers are given administrator profiles so that they can control the set up and disabling of normal user profiles.

Email and web browser protection
Some best practices for safe email transfer are implemented: email as zip or encrypted file when necessary, disable hyperlinks on email system, and avoid using generic email addresses and ensure the system has configured user accounts

Data recovery capability
Essential information and software-adequate backup facilities are available to ensure it can be recovered following a Cyber Incident. OT systems, which are vital to the safe navigation and operation of the ship, have backup systems to enable the ship to quickly and safely regain navigational and operational capabilities after a Cyber Incident.

Application software security (patch management)
Critical safety and security updates are provided to on-board systems. These updates or patches are applied correctly and in a timely manner to ensure that any flaws in a system are addressed before they are exploited by a Cyber Attack.

3.3.2 Threat Assessment

Threat assessment in Cyber Security is the process of identifying the origin, the motivation and the objective of the attacker, analyzing possible Cyber Threats/attacks and vulnerabilities, measuring the consequence and applying protective barriers to prevent threat or mitigate the impact (Bimco et al., 2017; Hatzivasilis et al., 2016; Marco Cesena et al., 2017).

In general, there are two categories of cyber- attacks, which may affect companies and ships:

- **untargeted attacks,** where a company or a ship's systems and data are one of many potential targets
- **targeted attacks**, where a company or a ship's systems and data are the intended target.

Untargeted attacks exploit over tools and techniques available on Internet. Examples of such tools are following

- **Malware:** Malicious software which is designed to access or damage a computer without the knowledge of the owner. There are various types of malware including trojans, ransomware, spyware, viruses, and worms. Ransomware encrypts data on systems until a ransom has been paid.
- **Social engineering:** A non-technical technique used by potential Cyber Attackers to manipulate insider individuals into breaking security procedures, normally, but not exclusively, through interaction via social media
- **Phishing**: Sending emails to a large number of potential targets asking for particular pieces of sensitive or confidential information. Such an email may also request that a person visits a fake website using a hyperlink included in the email.
- **Water holing**: Establishing a fake website or compromising a genuine website to exploit visitors.
- **Scanning**: Attacking large portions of the Internet at random.

Targeted attacks may be more sophisticated and use tools and techniques specifically created for targeting a company or ship. For example,

- **Brute force**: An attack trying many passwords with the hope of eventually guessing correctly.
- **DoS:** prevents legitimate and authorized users from accessing information, usually by flooding a network with data. A distributed denial of service (DDoS) attack takes control of multiple computers and/or servers to implement a DoS attack
- **Spear-phishing**: Like phishing but the individuals are targeted with personal emails, often containing malicious software or links that automatically download malicious software.
- **Subverting the supply chain:** Attacking a company or ship by compromising equipment, software or supporting services being delivered to the company or ship.

Such malicious events (attacks) imposes to shipping company the necessity to work proactively so to understand and mitigate Cyber Threats

The Table below is displaying group of attackers bundled with motivation between attack and objective of the attack. It is very crucial during threat evaluation not only to identify possible threats and potential attacks but to be able to understand who and why is behind those attacks

Table 1. Attackers categories, motivation and objective

Group	Motivation	Objective
Activists (including disgruntled employees)	Reputational damage Disruption of operations	Destruction of data Publication of sensitive data Media attention Denial of access to the service or system targeted
Criminals	Financial gain Commercial espionage Industrial espionage	Selling stolen data Ransoming stolen data Ransoming system operability Arranging fraudulent transportation of cargo Gathering intelligence for more sophisticated crime, exact cargo location, off vessel transportation and handling plans etc.
Opportunists	The challenge	Getting through Cyber Security defenses Financial gain
States State sponsored Organisations Terrorists	Political gain Espionage	Gaining knowledge Disruption to economies and critical national infrastructure

3.3.3 Training requirements

Cyber Threats raised where vulnerabilities in the system exist. Cyber Attack involves the attacker who in turn is motivated to trigger the attack in order to achieve a certain objective and the victim who in turn faces the consequences of the attack. Protective Barriers either in the form of technical protection or human awareness are set forward to prevent attack from impacting the system network components and cause negative consequences (Dnv Gl Maritime Advisory, 2016). A schematic flow of Cyber Threat mechanism is given in Figure 10.

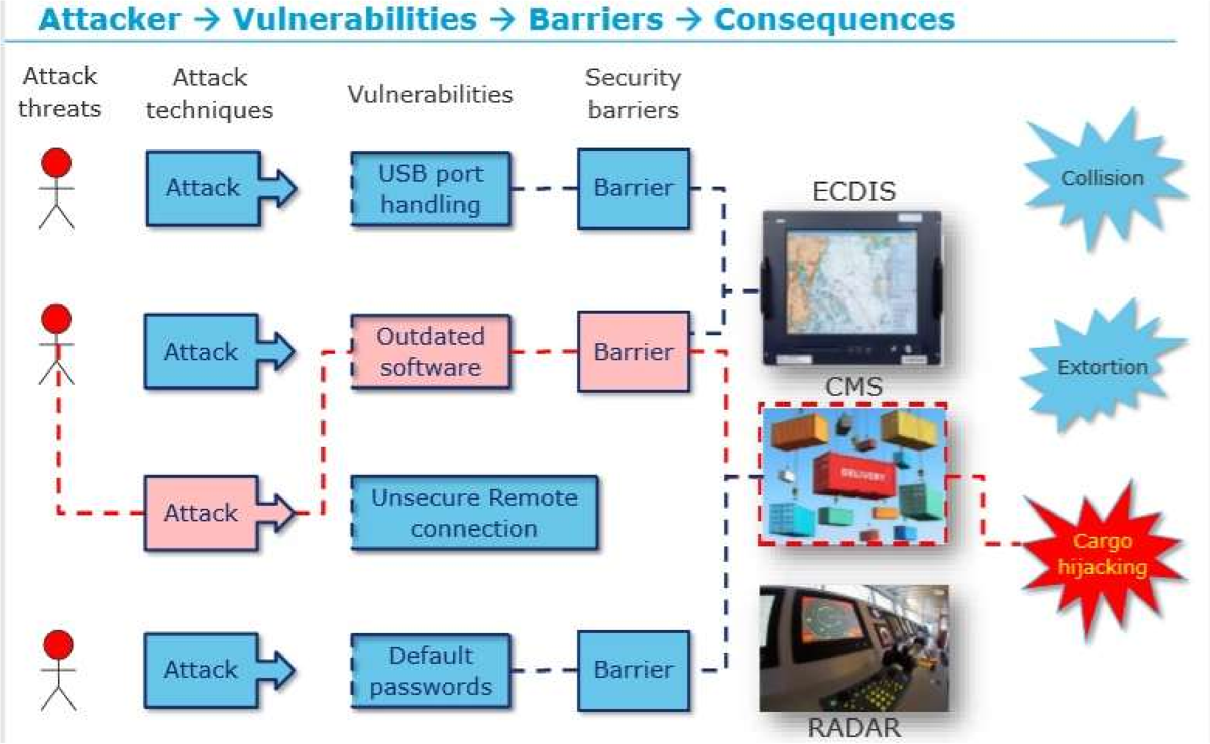


Figure 10. Flow of Cyber Threat mechanism

Along that Cyber Threat mechanism, training and awareness is the key supporting element and an important barrier along with technical and physical protection to an effective approach to cyber safety and security.

Shipping Company's staff have a key role in protecting IT and OT systems. Training and awareness should be tailored to the appropriate levels for:

- on-board personnel including the master, officers and crew
- shore-side personnel, who support the management and operation of the ship.

An awareness or training framework should be in place for all personnel, covering at least the following **risk factors and awareness aspects**:

1. risks related to emails and how to behave in a safe manner (examples are phishing attacks where the user clicks on a link to a malicious site);
2. risks related to Internet usage, including social media, chat forums and cloud-based file storage where data movement is less controlled and monitored;
3. risks related to the use of own devices (these devices may be missing security patches and controls, such as anti-virus, and may transfer the risk to the environment to which they are connected to);
4. risks related to installing and maintaining software on company hardware using infected hardware (removable media) or software (infected package);
5. risks related to poor software and data security practices where no anti-virus checks or authenticity verifications are performed;
6. safeguarding user information, passwords and digital certificates;
7. Cyber Risks in relation to the physical presence of non-company personnel, e.g., where third-party technicians are left to work on equipment without supervision;

8. detecting suspicious activity or devices and how to report if a possible Cyber Incident is in progress (examples of this are strange connections that are not normally seen or someone plugging in an unknown device on the ship network);
9. awareness of the consequences or impact of Cyber Incidents to the safety and operations of the ship.

Applicable personnel should be able to **identify the signals when a system has been compromised.** For example, training scenarios should trigger and evaluate user awareness aiming at the effective and efficient identification of hidden threats between applicable sings such as

- an unresponsive or slow to respond system;
- unexpected password changes or authorized users being locked out of a system;
- unexpected errors in programs, including failure to run correctly or programs running; unexpected or sudden changes in available disk space or memory;
- emails being returned unexpectedly;
- unexpected network connectivity difficulties;
- frequent system crashes;
- abnormal hard drive or processor activity;
- unexpected changes to browser, software or user settings, including permissions.

In the aforementioned context of risk awareness framework and signal identification, THREAT –ARREST will develop an advanced training programs incorporating emulation, simulation, serious gaming and visualization capabilities to adequately **train and evaluate** crew users with different types of responsibility and levels of expertise in **recognizing signals of possible Cyber Attacks**, **raising awareness on impact and consequences of attacks** while **following the necessary corrective actions** to defend high-risk Cyber Systems.

DANAOS will capitalize on the THREAT-ARREST platform which will deliver security training, based on a model-driven approach where Cyber Threat and training preparation (CTTP) models, specifying the potential attacks, the security controls of Cyber Systems against them, and the tools that may be used to assess the effectiveness of these controls while driving the training process, and align it (where possible) with operational cyber system security assurance mechanisms to ensure the relevance of training.

The THREAT-ARREST's maritime pilot objective is to increase the security awareness in shipping ICT systems' operators, and security attacks and help towards identifying new threats which jeopardize the operations of ICT systems in the Shipping Management industry.

4 General Legal and Regulatory Framework

4.1 Overview of the legal framework

The legal and regulatory framework related to the security and breach-related obligations should be integrated, at least to some extent, in the trainings to be developed in the context of the THREAT-ARREST project. Such framework can however be rather complex. Indeed, security and breach-related obligations imposed upon organizations derive from numerous sources, at both European and national level. They are also of various natures. The requirements may be imposed in legislative instruments, contracts, certifications, guidelines, internal policies, etc. It is therefore necessary for any organization prone to (cyber-)security threats to carefully train its employees on the applicable rules, which may vary depending on many factors, including the sector in which it is active.

The diagram below aims to provide a schematic overview of the security and breach-related obligations landscape.

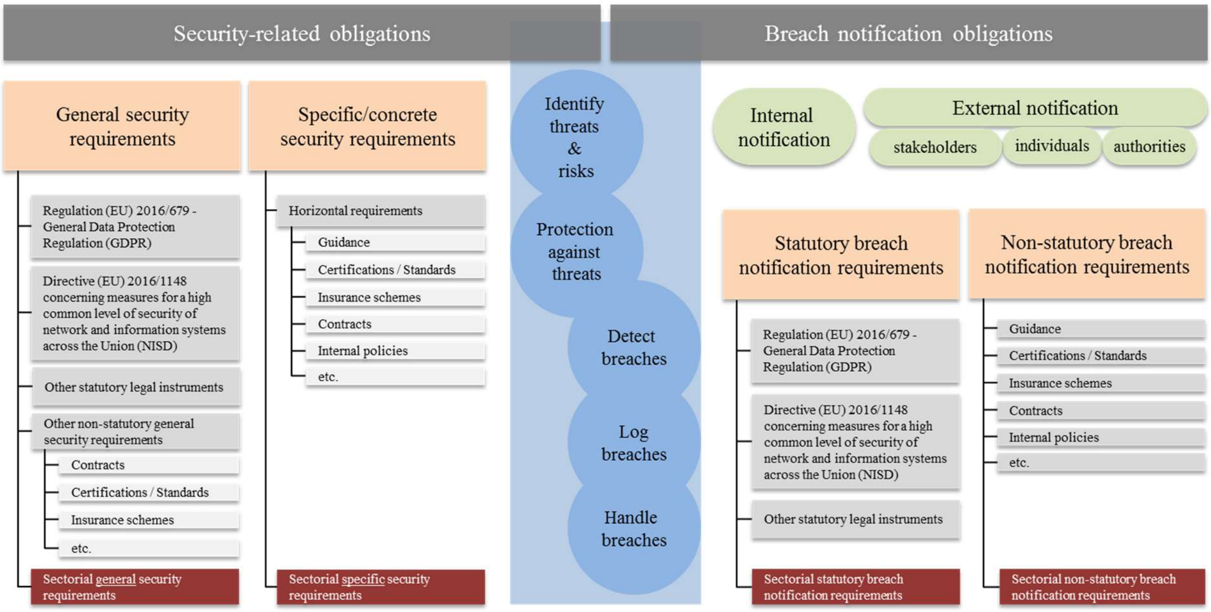

Security-related obligations
Breach notification obligations
General security requirements
Specific/concrete security requirements
Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR)
Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NISD)
Other statutory legal instruments
Other non-statutory general security requirements
Contracts
Certifications / Standards
Insurance schemes
etc.
Sectorial general security requirements
Horizontal requirements
Guidance
Certifications / Standards
Insurance schemes
Contracts
Internal policies
etc.
Sectorial specific security requirements
Identify threats & risks
Protection against threats
Detect breaches
Log breaches
Handle breaches
Internal notification
External notification
stakeholders
individuals
authorities
Statutory breach notification requirements
Non-statutory breach notification requirements
Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR)
Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NISD)
Other statutory legal instruments
Sectorial statutory breach notification requirements
Guidance
Certifications / Standards
Insurance schemes
Contracts
Internal policies
etc.
Sectorial non-statutory breach notification requirements

Figure 11. Overview of the security and breach-related requirements

The next sub-Sections aim to provide a preliminary introduction to the horizontal and non-sectorial obligations that may be applicable. These will however be further expanded on in the context of more detailed guidelines provided to the partners of THREAT-ARREST and included in deliverable D8.10.

4.2 Security-related obligations

Taking into consideration that a security incident calls into question the technical and/or organizational security measures in place, it is important to carefully integrate – notably in the context of trainings – the underlying security obligations and their infringement in case of a security incident.

There can be numerous sources of obligations imposing security measures to be implemented by an organization. Such sources may remain rather general and vague as to which specific measures are deemed appropriate. It follows from such generic security obligations that organizations would generally be required to:

- conduct a risk assessment (evaluate, manage and document the risks);

- carefully assess the security measures available on the market;
- continuously assess the adequacy of the implemented measures in light of the evolving risks and the available measures; and
- adequately reflect the security aspects in the various contracts between stakeholders.

Other sources may however be much more detailed and require or recommend an organization to put in place very specific security measures (see sub-Section 4.2.2 below).

4.2.1 General security requirements

Several legal instruments include requirements for organizations to put in place security measures (both technical and organizational) in order to protect data and/or systems. This is particularly the case of the General Data Protection Regulation (GDPR) and the Network and Information Security Directive (NISD). Both instruments remain however generic and do not detail the concrete measures to be implemented.

It follows that a security incident may lead to a breach of the core security-related obligations enshrined in such instruments. Accordingly, it is important to educate employees within an organization about the underlying rules in case of an incident.

4.2.1.1 General Data Protection Regulation (GDPR)

The requirements relating to security under the General Data Protection Regulation[6] (the "**GDPR**") will apply whenever "personal data" is processed. In the EU, the concept of "personal data" is rather wide-ranging. According to the GDPR, the concept refers to any information relating to an identified or identifiable natural person ('data subject'): *"An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"*.[7] The GDPR particularly expanded this concept to take account of the online environment.

Under the GDPR, any organization processing personal data must implement a wide range of measures to reduce the risk of non-compliance with the GDPR and to prove that it takes data governance seriously. Such measures create significant operational obligations and costs.

A general obligation is imposed upon data controllers[8] to adopt technical and organizational measures to meet the requirements set in the GDPR (and to be able to demonstrate that they have done so).[9] Operating a regular audit programme, implementing data protection by design and by default measures, conducting Data Protection Impact Assessments, appointing a Data Protection Officer, etc. are all measures considered to be in line with the data governance obligations, including the security-related requirements. Such measures must be reviewed and updated on a regular basis, taking into account the changing circumstances.[10]

Furthermore, it shall be borne in mind that the GDPR imposes a high duty of care upon data controllers in selecting their personal data processing service providers (data processors), which will require procurement processes and request-for-tender documents to be regularly assessed,

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1

[7] GDPR, art 4(1)

[8] The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

[9] GDPR, art 24

[10] GDPR, art 24(1)

in particular on the security aspects.[11] In the context of data-rich environments, data controllers should carefully reflect their security obligations in their respective agreements to be concluded with other actors, including processors and sub-processors.

The GDPR requires data controllers and processors to "*implement appropriate technical and organizational measures*".[12] Such measures shall take into account the following elements: (i) the state-of-the-art; (ii) the costs of implementation; (iii) the nature, scope, context, and purposes of the processing; and (iv) the risk of varying likelihood and severity for the rights and freedoms of natural persons.

When assessing the appropriate level of security, account shall be taken in particular of the risks presented by the processing, notably from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.[13] This entails that both data controllers and processors should continuously evaluate, manage and document those risks.[14]

Such risk-based approach, if carried out correctly, will not only lead to an effective and adequate security of the data processing, but may also be used to adhere to the accountability principle, which requires demonstrating compliance with the data protection principles and obligations laid down in the GDPR.

Finally, the GDPR indicates that adherence to an approved code of conduct or certification mechanism may be used as an element to demonstrate compliance with data governance obligations[15] as well as security requirements.[16] Currently, such codes of conduct or certification mechanisms are being developed throughout the EU. Such development can only be encouraged in order to provide practical assistance to organizations.

4.2.1.2 Network Information Security Directive (NISD)

The (minimal harmonization) Network and Information Security Directive[17] (the "**NIS Directive**" or "**NISD**") was adopted on 6 July 2016 to address the increasing challenges in relation to Cyber Security. This EU legislation aims to cultivate a common approach across the EU to address any socio-economic damage that may be caused by attacks on the network and information systems of operators of essential services and digital service providers.

Taking into account its nature as a Directive, the NIS Directive had to be implemented by the EU Member States into their national laws by May 2018.[18] It is therefore required to carefully consider the national obligations, which may be particularly relevant to a particular organization, depending on whether it qualifies as an Operator of Essential Services ("**OES**") or a Digital Service Provider ("**DSP**"), and depending on the sector in which it is active.

More specifically, the distinction between OES and DSP is of particular importance and may be summarized as follows:

[11] GDPR, art 28
[12] GDPR, art 32
[13] GDPR, art 32(2)
[14] Commission de la protection de la vie privée, 'Big Data Rapport' (CPVP 2017) 58 <https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Rapport_Big_Data_2017.pdf> accessed 18 December 2018
[15] GDPR, arts 24(3) and 28(5)
[16] GDPR, art 32(3)
[17] Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1
[18] Some countries are however late in transposing the requirements of the NISD.

Table 2. Difference between OES and DSP

Operators of Essential Services (OES)	Digital Service Providers (DSP)
Article 5 of the NIS Directive defines an essential service as "*a service essential for the maintenance of critical societal and/or economic activities depending on network & information systems, an incident to which would have significant disruptive effects on the service provision*." EU Member States had to identify the operators of essential services established on their territory by 9 November 2018 based on several criteria, and notably whether or not an incident would have significant disruptive effects on the provision of that service. According to the NISD, operators active in the following sectors may be identified in each Member State: • energy, • transport, • banking, • stock exchange, • healthcare, • utilities, or • digital infrastructure.[19]	A digital service is described as "*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*".[20] In contrast with the OES, which are identified by each EU Member State, online businesses must self-assess whether they are targeted by the rules of the NIS Directive, and in particular whether they fall within the following three different types of digital services: • online marketplaces, • online search engines, or • cloud computing services.[21]

In the event that the NISD (and the implementing national rules) applies to a particular organization, the latter will have to (i) interact with new key actors; (ii) implement security measures; and (iii) notify security incidents.

With regard to the security measures, the NISD includes generic security obligations by requiring OES and DSP to take appropriate and proportionate technical and organizational measures to manage the risks posed to the networks and information systems which they use for the provision of their services, and to prevent and minimize the impact of incidents affecting the security of such network and information systems.[22] The security measures shall take into account the state-of-the-art, to ensure a level of security of network and information systems adequate to the risk.

[19] NIS Directive, Annex II

[20] NIS Directive, art 4(5). A digital service provider without an establishment in the EU but providing services within the EU must appoint a representative. This representative will need to be established in one of the EU Member States where the digital services concerned are offered. In that case, the digital service provider shall be deemed to be under the jurisdiction of the Member State where the representative is established (NIS Directive, art 18(2)). Micro and small enterprises (as defined in Commission Recommendation 2003/361/EC) do not fall under the scope of the Directive.

[21] NIS Directive, arts 4(17)-(19)

[22] NIS Directive, arts 14 and 16

4.2.1.3 Other general security requirements

In addition to the GDPR and the NISD, other legislative instruments may apply, which may be sector-focused, and impose generic security requirements.

For instance, in the electronic communications sector, several EU Directives, transposed in the national laws of the (currently) 28 Member States, provide for security obligations – such as for instance:

- The e-Privacy Directive[23]: it is required that providers of electronic communications services take appropriate technical and organizational measures to safeguard the security of their services, where necessary in conjunction with the provider of the public communications network.

- The Framework Directive[24]: it complements the e-Privacy Directive by requiring providers of publicly available electronic communication networks and services to take appropriate measures to manage the risks posed to the security of the networks and services. The Directive also requires the providers to guarantee the integrity of their networks and continuity of supply.

- The Radio Equipment Directive[25]: privacy and data protection requirements apply to terminal equipment attached to public telecommunication networks. Radio equipment within certain categories or classes shall incorporate safeguards to ensure that the personal data and privacy of users and subscribers are protected.

Moreover, the generic obligation to put in place technical and organizational security measures may be imposed through other means such as by way of c**ontracts**: by way of example, contractual arrangements between parties may include clauses such as the following:

> *"The Service Provider shall ensure that it has in place appropriate technical and organizational measures, reviewed and approved by Company, having regard to the state of technological development and the cost of implementing any measures."*

In the same vein, generic security requirements may be imposed by insurers in their **insurance schemes** or included in **certifications / standards**.

4.2.2 Specific / concrete security requirements

In some cases, organizations may be bound by horizontal obligations to implement specific and concrete security requirements.

Such obligations are generally not included in strictly legislative instruments as the legislative process does not tend to keep pace with technological evolution.

This being said, while the GDPR does not detail the security measures that can or should be put in place, it nonetheless provides the following specific suggestions for what types of security measures might be considered “appropriate to the risk”:

[23] Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector [2005] OJ L 201/37 (e-Privacy Directive)

[24] Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services [2002] OJ L 108/33 (Framework Directive)

[25] Directive 1999/5/EC of the European Parliament and of the Council on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity [1995] OJ L 91/10 (Radio Equipment Directive)

1. the pseudonymisation and encryption of personal data;
2. the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services;
3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.[26]

The NISD, on its part, does not provide such types of examples and remains very generic.

The specific obligations that may be imposed upon an organization can be found in other, more or less binding, instruments. A few examples of such instruments are:

- **Guidance**: numerous authorities, both at EU and national level, have published non-binding guidance on security aspects, with the aim of providing specific recommendations on the security measures that an organization should consider implementing. These guidance documents may focus on specific technologies (e.g. cloud computing, big data, IoT, etc.), on particular sectors (e.g. telecommunications, finance, etc.), as well as on certain key topics (e.g. privacy, certification, e-government, biometrics, cryptocurrencies, etc.).

- **Certifications / Standards**: in some cases, an organization may decide to become certified and to follow national or international standards. Relying on standards and certification schemes facilitates demonstrating compliance with legal requirements, including security requirements. By relying on existing schemes, such as for instance the ISO/IEC 27000 series issued by the International Standards Organization ("**ISO**") and the International Electrotechnical Commission ("**IEC**"), an organization implements measures that are specifically listed and imposed. This notably allows demonstrating to the regulator and to customers/users that their systems are adequate, or at least that measures and processes have been implemented in terms of security. In addition to the ISO/IEC standards, several other standards development organizations have created and are currently developing or updating standards: e.g. the Organization for the Advancement of Structured Information Standards (OASIS), the International Telecommunication Union – Telecommunications sector (ITU-T), the World Wide Web Consortium (W3C), etc.

- **Insurance schemes**: in many cases, an organization will seek an insurance to cover its Cyber Risks. In such context, insurers generally impose the implementation of specific security measures and calculate the insurance premium on the basis of the particularities of the company, including its Cyber Risk and the implemented measures. Accordingly, the organisation must carefully assess its obligations under its insurance agreements in order to ensure that it will be covered in case of a Cyber Attack.

- **Contracts**: commercial contracts usually include data protection, security and/or incident-related clauses. In such context, depending on the relationship, the qualities of the parties and the subject-matter of the agreement, a contract may impose more or less detailed security requirements. The following example aims to provide an illustration of a detailed clause regarding the security measures that may be imposed upon an organization:

[26] GDPR, art 32(1)

> *The Service Provider commits to implementing and respecting the appropriate technical and organizational security measures, which are necessary for the protection of the data, including but not limited to personal data, against amongst others destruction, loss, alteration, unauthorized disclosure or unauthorized access. The Service Provider shall describe these measures in a security policy.*
> *The Service Provider shall communicate its security policy mentioned above without delay to the Client upon the latter's simple request.*
> *The minimum appropriate technical and organizational security measures the Service Provider must take are set out in Annex X.*

- **Internal policies**: in order to effectively comply with its various obligations, it is necessary for an organization to ensure that internal rules (policies, standards, procedures, etc.) are adopted and enforced within the organization, including in relation to security. Such documents may include detailed security measures, both organizational and technical.

4.3 Breach notification obligations

In addition to educating and training an organization's personnel in relation to the security obligations and their related violation in case of a security incident, it is also important to train employees about the specific notification requirements in case of an incident or breach.

The present Section therefore focuses on the applicable legal obligations, which derive from the GDPR, but also, where relevant, from other legal instruments at different levels.

4.3.1 Statutory breach requirements

Several legal instruments include requirements for organizations to put in place certain measures to detect and manage breaches, but also to notify such breaches to authorities, affected individuals, and/or other concerned stakeholders. This is particularly the case for the GDPR and the NIS Directive.

4.3.1.1 General Data Protection Regulation (GDPR)

The GDPR requires the notification within 72 hours of "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.*"[27]

It follows from such definition that many types of incidents will be considered as data breaches within the meaning of the GDPR. It goes without saying that the occurrence of breaches in the context of new technologies is not hypothetical. This will require abiding by the strict obligations related to the notification of such incidents to the adequate data protection authorities across the EU (as well as to possible other authorities across the world in certain large breaches).

The breach notification obligation under the GDPR evidently only applies in case of a breach of personal data. It is therefore essential to carefully assess, in the event of an incident, the nature of the data exposed. If such assessment shows that no personal data has been affected, in principle no data breach notification is required under the GDPR. In this respect, it could

[27] GDPR, arts 4(12) and 33

reasonably be advocated that a breach of anonymized data or encrypted data, the key to which cannot be retrieved by a third-party, should not need to be notified under the GDPR.

Therefore, appropriate technical and organizational measures should be implemented to be able to detect promptly whether a personal data breach has taken place and to immediately inform the supervisory (data protection) authority and the affected individuals, if needed.[28] Such measures include the keeping of adequate logs, which facilitates a swift and efficient forensics investigation in case of an incident.

A personal data breach notification by a data controller to a supervisory (data protection) authority must at least mention the following information:[29]

1. The nature of the breach, including the categories and approximate number of individuals as well as personal data records affected;
2. The name and contact details of the data protection officer or any other contact point that could provide more information;
3. The likely consequences of the breach; and
4. The measures (proposed to be) taken by the data controller to address the breach, including any measures to mitigate its negative effects.

The Article 29 Working Party (the predecessor of the European Data Protection-board) focuses on an assessment of risks – so precise numbers are not needed, but factors relevant to risk should be highlighted (i.e. special categories of data, vulnerable groups). It also suggests that if the breach is caused by a processor – and if the processor has caused a breach for multiple controllers – that the controller "may find it useful to name its processor [in the notification] if it is at the root cause".[30]

In case it proves impossible to provide the abovementioned information simultaneously within 72 hours, the GDPR allows providing such information in different phases.[31] However, the notification should indicate the reasons for the deferment, and the missing information should be provided without further undue delay.[32]

The communication to the affected individuals must detail in clear and plain language the nature of the personal data breach, recommendations to mitigate possible adverse effects, as well as the information listed under (ii), (iii) and (iv) above.[33]

In line with the principle of accountability, further elaborated in the sub-Section dedicated to the GDPR security requirements (see above), the data controller must document any personal data breach as well as the corrective measures taken in order to allow the supervisory (data protection) authority to assess compliance with the data breach notification obligations.[34]

4.3.1.2 Network Information Security Directive (NISD)

The NISD requires OES to notify the national competent authority or the Computer Security Incident Response Team CSIRT, without undue delay, of incidents having a significant impact on the continuity of the essential services they provide.[35] Similarly, DSP are required to notify

[28] GDPR, Recital 87
[29] GDPR, art 33(3)
[30] Article 29 Data Protection Working Party, 'Guidelines on Personal data breach notification under Regulation 2016/679' (2018) WP250rev.01, 15
[31] GDPR, art 33(4)
[32] GDPR, Recital 85
[33] GDPR, art 34(2) and Recital 86
[34] GDPR, art 33(5)
35 NIS Directive, art14(3)

the national competent authority or the CSIRT without undue delay of any incident having a substantial impact on the provision of a digital service (as identified in sub-Section 4.2.1.2 above) offered within the EU.[36]

According to the NISD, the factors to be considered when determining whether the impact of an incident is significant are the following:

Table 3. Factors to determine the significance of an incident

OES	DSP
• the number of users affected by the incident; • the duration of the incident; and • the geographical spread of the incident.[37]	• the number of users affected by the incident; • the duration of the incident; • the geographical spread of the incident; • the extent of the disruption of the service; and • the extent of the impact on economic and societal activities.[38]

In addition to the above general rules included under the NISD, the following clarification documents have been published:

Table 4. Overview of EU guidelines related to NISD notification requirements

OES	DSP

[36] NIS Directive, art16(3)
[37] NIS Directive, art 14(4)
[38] NIS Directive, art 16(4)

• "Reference document on Incident Notification for Operators of Essential Services – Circumstances of notification"[39], published by the NIS Cooperation Group in February 2018.[40] Such document details the incident notification scheme for OES but also the parameters used to measure the impact of incidents. It also examines the intricacies of cross-border situations and the interplay of the NISD with notification requirements in other legislations (including the GDPR). • "Guidelines on Notification of Operators of Essential Services incidents – Formats and procedures"[41], published by the NIS Cooperation Group in May 2018.[42] Such document provides (non-binding) guidance to national competent authorities and CSIRTs with regard to formats and procedures for the notification of incidents by OES, to facilitate alignment in the implementation of the NIS Directive across the EU.	• Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of the [NIS Directive] as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.[43] Such document notably clarifies four situations in which DSP are required to notify the relevant national competent authority or CSIRT, notably: (i) if the digital service is unavailable for more than 5 million user-hours in the EU; (ii) if more than 100,000 users in the EU are impacted by a disruption; (iii) if the incident has created a risk to public safety, public security or of loss of life; or (iv) if the incident has caused material damage of more than €1 million. • "Guidelines on notification of Digital Service Providers incidents - Formats and procedures", published by the NIS Cooperation Group in June 2018. Such document provides non-binding technical guidance to national competent authorities and CSIRTs with regard to formats and procedures for the notifications of incidents by DSP, to facilitate alignment in the implementation of the NIS Directive across the EU.

[39] NIS Cooperation Group, 'Reference Document on Incident Notification for Operators of Essential Services. Circumstances of Notification' (European Commission 2018) <http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53644> accessed 17 October 2018

[40] The NIS Cooperation Group is established by the NISD and started its work in February 2017. It gathers national competent authorities responsible for Cyber Security and is composed of representatives of Member States, the European Commission, and ENISA. The NIS Cooperation Group facilitates the dialogue between different bodies responsible for Cyber Security in the EU. It represents a shared space where common Cyber Security challenges are discussed and coordinated policy measures are agreed upon.

[41] NIS Cooperation Group, 'Guidelines on Notification of Operators of Essential Services Incidents. Formats and Procedures' (European Commission 2018) <http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53677> accessed 17 October 2018

[42] The NIS Cooperation Group is established by the NISD and started its work in February 2017. It gathers national competent authorities responsible for Cyber Security and is composed of representatives of Member States, the European Commission, and ENISA. The NIS Cooperation Group facilitates the dialogue between different bodies responsible for Cyber Security in the EU. It represents a shared space where common Cyber Security challenges are discussed and coordinated policy measures are agreed upon.

[43] Commission Implementing Regulation (EU) 2018/151 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact [2018] OJ L 26/48

	• "Incident notification for DSPs in the context of the NIS Directive"[44] report published by ENISA on 27 February 2017. Such report includes a comprehensive guideline on how to implement incident notification for DSPs.

In case an operator of essential services depends on a digital service provider for the provision of such essential services, any significant impact on the continuity of those services due to an incident affecting the digital service provider must be notified by that operator.[45] The NIS Directive remains silent as to whether, in such circumstances, the digital service provider is obliged to notify such incident to the operator of essential services. It is therefore to be expected (and highly recommended) that the operator of essential services would require such notification by the digital service provider contractually.
The notified national competent authority or CSIRT shall inform other Member States affected.[46] In such case, the national competent authority, the CSIRT and the single point of contact shall ensure that the service provider's security and commercial interests are safeguarded and that the information provided remains confidential. The national competent authority or CSIRT may also decide – after consultation with the notifying operator – to inform the public, where such public awareness would be necessary to prevent or manage an incident.[47]

Pursuant to the NIS Directive, the EU Member States may not impose any further notification requirements on DSP, unless for the protection of essential State functions and for the preservation of law and order.[48]

4.3.1.3 Other statutory breach notification requirements

In addition to the GDPR and the NISD, other legislative instruments may apply, which may be sector-focused, and impose breach-related obligations.

For instance, in the electronic communications sector, the Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector[49] (the "**e-Privacy Directive**") was the first EU-wide legislative instrument to impose data breach notification obligations. Pursuant to the Directive, publicly available electronic communication service providers ("**PECS providers**") must, if they suffer a breach of security that leads to personal data being lost or stolen, inform the national authority and, in certain cases, the subscriber or individual.[50]

[44] European Union Agency for Network and Information Security, 'Incident Notification for DSPs in the Context of the NIS Directive. A Comprehensive Guideline on How to Implement Incident Notification for Digital Service Providers, in the Context of the NIS Directive' (ENISA 2017) <https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive> accessed 19 December 2018

[45] NIS Directive, art 16(5)

[46] NIS Directive, arts 14(5) and 16(6)

[47] NIS Directive, arts 14(6) and 16(7)

[48] NIS Directive, art 16(10) *juncto* art 1(6)

[49] e-Privacy Directive

[50] e-Privacy Directive, art 4(3)

Regulation 611/2013 on the measures applicable to the notification of personal data breaches (the "**Data Breach Notification Regulation**") lays down the circumstances in which PECS providers must notify personal data breaches, the format of such notification and the procedure to follow.[51] Taking into account its nature as a Regulation, the Data Breach Notification Regulation has direct effect in all EU Member States, rendering any national implementation measures unnecessary.[52]

The e-Privacy Directive is currently being reviewed in the framework of the EU Digital Single Market ("**DSM**") strategy. In this respect, the EU Commission held a public consultation, the report of which was made available in August 2016.[53] In its 'Opinion 03/2016 on the evaluation and review of the ePrivacy Directive', the Article 29 Working Party notably recommended to remove the provisions relating to breach notification from the e-Privacy Directive given their "overlap" with the breach notification obligations under the GDPR (see above).[54] On 10 January 2017, the EU institutions adopted a draft e-Privacy Regulation, which would be directly applicable in all EU Member States.[55] The latest version of the draft does not contain a data breach notification obligation as such, which is justified by the fact that the GDPR will apply to PECS providers.[56]

4.3.2 Non-statutory breach notification requirements

In addition to the statutory legal requirements for an organisation to notify a breach, similar obligations may exist in other non-statutory instruments, but which may nonetheless be binding upon the organisation and/or its personnel. A few examples of such instruments are:

- **Guidance:** numerous authorities, both at EU and national level, have published guidance documents in relation to breach notification requirements in different contexts (e.g. privacy and data protection, telecommunications, etc.). Such guidance may be useful in order to determine whether or not the organisation is under any notification obligation, but also on the practical aspects of such notification to the authorities, affected individuals, and other stakeholders.

- **Certifications / Standards:** in some cases, an organisation may decide to become certified and to follow national or international standards. Some standards relate specifically to incident and breach management. For instance, among the ISO/IEC standards, it is worth mentioning ISO/IEC 27035 (for incident management), ISO/IEC 27031 (for ICT readiness for business continuity) or ISO/IEC 22301 (for business continuity management systems (BCMSs)).

- **Insurance schemes:** in case an organisation is insured for its Cyber Risks, the insurer may impose strict notification obligations and incident management procedures in order to ensure that the organisation takes the necessary measures to inform within strict deadlines the insurer, but also other stakeholders, about any security incident.

[51] Commission Regulation (EU) 611/2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications [2013] OJ L 173/2

[52] Davinia Brennan, 'New Rules on Breach Notification by Telecoms and ISPs – Clarity at Last?' (2013) 14(1) P & DP 4

[53] Summary report available online at <https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-evaluation-and-review-eprivacy-directive>

[54] Article 29 Data Protection Working Party, 'Opinion 03/2016 on the evaluation and review of the ePrivacy Directive' (2016) WP 240, 19

[55] Commission, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC' (Regulation on Privacy and Electronic Communications), COM (2017) 10 final

[56] Whereas GDPR focuses on general uses of personal data, the upcoming e-Privacy Regulation will supplement the GDPR with additional rules targeted at electronic communications services, the use of cookies, online behavioural advertising, direct marketing and machine-to-machine communications.

- **Contracts:** commercial contracts usually include incident notification clauses. Such clauses may be legally required in certain cases, such as for instance in the context of a controller-processor relationship within the meaning of the GDPR. In such instances, one party must inform the other party of a security incident. The provisions may impose strict formats, content and deadlines.

- **Internal policies:** in order to effectively comply with its various obligations, it is necessary for an organisation to ensure that its internal rules (policies, standards, procedures, etc.) are adopted and enforced within the organisation, including in relation to the notification of breaches. Such documents may include detailed measures to be followed by different levels and departments of the organisation.

5 Sectorial Legal and Regulatory Framework

5.1 Smart Energy Systems Pilot

The growing digitalization of the energy sector entails numerous challenges, including the need to ensure appropriate and effective Cyber Security for producers, operators, suppliers, other market participants and consumers. Due to the nature of the energy sector, the legal and regulatory framework for security and breach-related obligations is extensive, complex and dispersed across various legal and other instruments. To gain insight into the range of security and breach-related obligations applicable to the Smart Energy Systems Pilot, it is therefore important to delineate the particular field of the energy sector in which the Pilot operates.

We understand that the Smart Energy Systems Pilot deals with household electricity generation and consumption by pairing residential solar power systems with battery storage and smart home monitoring systems. It follows that the Pilot operates in the electricity sector and deals in particular with smart grids and smart metering systems.

5.1.1 General security and breach-related requirements

The above general overview of the legal and regulatory framework on security and breach-related demonstrated the existence of both very general and very specific obligations. It was established that two of the most important instruments imposing such obligations across all sectors of the economy are the GDPR and the NIS Directive. Although the present Section will not go into detail on the general obligations that may follow from the GDPR and the NIS Directive, the following high-level assessment can be made.

First, we note that the Smart Energy System Pilot will be required to comply with the security and breach-related requirements imposed by the GDPR. While this depends on whether or not the Pilot processes personal data, but in light of the broad definition of personal data, it seems highly likely that the GDPR will apply.

Second, as regards applicability of the NIS Directive it is considered unlikely that the Pilot will be considered an OES under this Directive. However, as the Smart Energy Systems Pilot makes use of the SIDE Edge IoT platform, which in turn relies on SIDE Cloud infrastructure, it may be considered a DSP providing cloud computing services. This will depend on whether the SIDE Cloud infrastructure is developed and provided by the Pilot itself, or whether the cloud computing services are entirely offered by a third-party. This requires a thorough assessment of the SIDE Cloud infrastructure and how this is provided to the customers of the Pilot.

The rest of this Section will focus on a number of sector-specific obligations and guidelines applicable to the Pilot.

5.1.2 Sector-specific security and breach-related requirements

First and foremost, it should be noted that the relevant obligations and/or guidance can emanate from different levels, including (but not limited to) the EU level and the national level.

5.1.2.1 EU level

At EU level, various regulations (directly) and directives (indirectly through implementation at national level) impose obligations related to the security of the electricity network in general and smart grids and smart metering systems in particular.[57] Many of these security-related

[57] We refer, among others, to Directive 2005/89/EG of the European Parliament and Council of 18 January 2006 concerning measures to safeguard security of electricity supply and infrastructure investments and to Directive 2009/72/EC of the European

obligations are however imposed on transmission system operators and distribution system operators and therefore do not fall directly on the Smart Energy Systems Pilot.

Important in this respect is Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. That Directive establishes a common procedure for identifying European critical infrastructure, such as power plants and transmission infrastructure, and a common approach to the assessment of the need to improve the protection of such infrastructures. It also focuses on the energy sector, including on infrastructures and facilities for generation and transmission of electricity in respect of supply electricity.

Particularly relevant for the Smart Energy Systems pilot is Directive 2004/22/EC of the European Parliament and of the Council of 31 March 2004 on measuring instruments, which applies to the devices and systems with a measuring function defined in the instrument-specific annexes concerning, among others, active electrical energy meters. It stipulates the essential requirement that measuring instruments must provide "*a high level of metrological protection in order that any party affected can have confidence in the result of measurement*", and that these must be "*designed and manufactured to a high level of quality in respect of the measurement technology and security of the measurement data*".

However not all requirements are strict legal requirements. A number of important non-binding recommendations and guidelines have also been made at EU level, including (but not limited to):

- "The Proposal of December 2013 for a list of security measures for smart grids" by the Smart Grid Task Force Expert Group 2 on Cyber Security. The European Network and Information Security Agency (**ENISA**) has drawn up security measures to help smart grid providers improve the infrastructures' cyber resilience. The proposal for a list of security measures for smart grids contains 45 security measures and the mapping of the identified security measures to potential threats;

- "The Data protection impact assessment template for smart grids and smart metering systems", adopted on 13 December 2018. That template is destined for data controllers that are smart grid operators managing or initiating smart grids or smart metering systems, as well as those introducing changes to existing smart grid architecture platforms. Since the collection and usage of personal data is one of the key business enablers for smart grid operators, the inherent risks to the rights and freedoms of natural persons must be properly assessed and mitigated and the rules for collecting personal data should be established, in particular with regard to proportionality of collection to the purpose of processing and legal basis;

- "The Report SG-CG/M490/H on Smart Grid Information Security" of December 2014 by the CEN-CENELEC-ETSI Smart Grid Coordination Group. This report of the European standardization organizations CEN, CENELEC and ETSI was prepared under a mandate from the European Commission and the European Free Trade Association. The objective of the report is to support smart grid deployment in Europe by providing information security guidance and standards to smart grid stakeholders. In order to

Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC.

support Smart Grid deployment with security by design, a set of recommendations has been derived which is closely linked to ENISA's set of recommendations.

In addition the existing framework, we note that at EU level, several proposals that may entail additional security and breach-related obligations are currently on the agenda. Some of the most relevant proposals are:

- The Proposal for a Directive of the European Parliament and of the Council on common rules for the internal market in electricity (recast), in which a new provision on smart metering functionalities would require smart metering systems to be implemented with, among others, due regard of "*the best available techniques for ensuring the highest level of Cyber Security protection*";

- The Proposal for a Regulation of the European Parliament and of the Council on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC, the main objective of which would be to improve the identification of possible crisis situations, the preparation of crisis-management plans and the handling of a crisis situation in the electricity sector and which would complement the NIS Directive ensuring that Cyber Incidents are properly identified as a risk, and the measures taken to deal with them are properly reflected in the risk-preparedness plans;

- The Proposal for a Regulation of the European Parliament and of the Council on the internal market for electricity (recast). Article 55 of this proposed regulation would introduce the power for the European Commission to adopt delegated acts concerning the establishment of network codes on a variety of topics, including on the topic of Cyber Security. In this context, specific rules are being developed as a matter of priority through a network code as foreseen in this revised regulation, which will take account of new risks resulting from the digitalization of energy systems. In an interim report of December 2017 "Recommendations for the European Commission on Implementation of a Network Code on Cyber Security", the Smart Grids Task Force Expert Group 2 on Cyber Security has prepared the ground for the network code on energy-specific Cyber Security.

5.1.2.2 UK level

Security and breach-related obligations and/or guidelines are however not only imposed or issued at EU level, but also emanate from the national level. This includes obligations resulting from the transposition into national law of obligations contained in the EU directives mentioned above.

While this high-level assessment does not aim to provide an exhaustive overview of all relevant obligations at national level, the following standards are particularly relevant for the Smart Energy Systems Pilot, as it operates in the UK:

- "Commercial Product Assurance Security Characteristic Smart Metering – Electricity";
- "Commercial Product Assurance Security Characteristic Smart Metering – Communications Hub";
- "Commercial Product Assurance Security Characteristic Smart Metering – HAN Connected Auxiliary Load Control Switch".

Commercial Product Assurance ("**CPA**") evaluates off-the-shelf products and their developers against published security and development standards. The above documents all describe the features, testing and deployment requirements necessary to meet CPA certification for electricity smart metering equipment security products. They are aimed at a wide audience including vendors, system architects, developers, evaluation and technical staff operating within the security arena. The documents describe both the purpose and scope of the relevant security product, general security characteristics and specific measures required to prevent or hinder attacks. Typically, these mitigating measures are grouped into the three requirement categories design, verification and deployment

5.2 Healthcare Cyber Security Training

The increasing digitalization of the society undeniably also has an impact on the healthcare sector, and more precisely on the way healthcare professionals or governments interact amongst themselves and with patients. An example thereof are healthcare organizations introducing apps which patients can use to view and schedule appointments, see a summary of their patient history, review prescriptions and, most importantly, video connect to their providers directly from a smart device. Another example would be the eHealth platforms several governments have set up in order to communicate with citizens concerning health related issues.

The (cyber-)security legal and regulatory requirements relevant to the healthcare industry are governed by, on the one hand, general security-related legal instruments, which are sometimes explicitly declared applicable to the healthcare industry, and on the other hand, concrete security requirements and recommendations emitted by authorities at different levels.

Any (cyber-)security training should, to a certain extent depending on the target audience, take into account such legal requirements and recommendations. The present Section intends to give an illustrative overview of some of the instruments relevant to the healthcare sector.

5.2.1 General security and breach-related requirements

5.2.1.1 GDPR

As discussed in sub-Section 4.2.1.1 above, the GDPR applies to the processing of personal data in the context of the activities of an organisation established within the EU, or to the processing of personal data of individuals in the EU where such processing relates to the offering of goods or services to those individuals or the monitoring of their behavior within the EU. As such, the GDPR has no sectorial approach, in the sense that it may apply horizontally and without distinction to organizations across different sectors and industries.

This being said, the GDPR does regulate the processing of sensitive personal data more attractively. The processing of such types of data is restricted and prohibited in most cases. Accordingly, in order to process such special categories of data, the data controller must find a proper legal ground exhaustively listed in the GDPR, but must also apply higher standards in terms of security and cyber management given the risks for individuals should there be a breach of sensitive data.

The GDPR includes the following notions and definitions particularly relevant to the pilot:

Table 5. Notions and definitions related to sensitive personal data

Concept	Definition / clarification
"**Special categories of personal data**"	"personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and (…) genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" (Article 9(1) GDPR)
"**Data concerning health**"	"personal data related to the physical or mental health of a natural person, including the provision of Healthcare services, which reveal information about his or her health status" (Article 4(15) GDPR)
"Genetic data"	"personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question" (Article 4(13) GDPR)
"Biometric data"	"personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data" (Article 4(14) GDPR)

Therefore, the Pilot will be required to comply with the heightened security and breach-related requirements imposed by the GDPR, which have been dealt with in Section 4.3 above.

5.2.1.2 NIS Directive

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (the "**NIS Directive**") was adopted to address the increasing challenges in relation to Cyber Security at EU level.

Further information on the requirements of the NIS Directive has been given in sub-Section 4.2.1.2 above and will be made available in Deliverable D8.10.

It is however important to note in the context of the healthcare Pilot that Annex II of the NIS Directive explicitly covers the health sector, targeting "Healthcare settings (including hospitals and private clinics"[58] as potential "operators of essential services" to which the requirements of the NIS Directive would apply.

In light of the information currently available, it is however unlikely that the Smart Shipping Management Pilot would be qualified as an operator of essential services under the NIS Directive.

[58] Healthcare providers as defined in point (g) of Article 3 of Directive 2011/24/EU of the European Parliament and of the Council.

5.2.2 Sector-specific security and breach-related requirements

5.2.2.1 Medical Devices Regulation

The Medical Devices Regulation[59] (or MDR) lays down general security requirements for medical devices[60], including software as a medical device. Software as a medical device ranges for example from software that allows a smartphone to view images obtained from a magnetic resonance imaging (MRI) medical device for diagnostic purposes to Computer-Aided Detection (CAD) software that performs image post-processing to help detect breast cancer. Increasingly, this software, and medical devices more generally, are under Cyber Threat. It goes without saying medical devices hold an enormous amount of often sensitive data. Breaches following a Cyber Attack could therefore have considerable consequences.

Medical devices classified as such have to bear a CE marking indicating conformity with the standards defined in Annex I requiring, among others, (i) medical devices do not compromise the clinical condition or the safety of patients when used in the intended way and (ii) risks are minimized.

Furthermore, pursuant to article 17.2 of said Annex I, for devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of information security.

Finally, with respect to breach notification requirements, apart from other notification obligations applicable to the healthcare sector as a whole, notably pursuant to the GDPR and NISD, article 87 (1) of the Medical Devices Regulation specifically imposes manufacturers of medical devices available on the Union market, the obligation to report to the relevant competent authorities any serious incidents involving those devices. A 'security incident' is defined by the MDR as any incident that directly or indirectly led, might have led or might lead to either (i) the death of a patient, user or other person; (ii) the temporary or permanent serious deterioration of a patient's, user's or other person's state of health or (iii) a serious public health threat.

5.2.2.2 Security and Resilience in eHealth Infrastructures and Services – ENISA Guidance

ENISA published on 18 December 2018 an extensive report on eHealth entitled "Security and Resilience in eHealth Infrastructures and Services"[61], with the aim of investigating the approaches and measures Member States take to protect critical healthcare systems, having as a main goal improved healthcare and patient safety.

More particularly, this ENISA report analyzes:

- The policy context in Europe and the legislation of the Member States
- The perception of the Member States on critical assets in eHealth infrastructures
- The most important security challenges
- The most common security requirements

[59] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC.

[60] Medical devices in the sense of the Regulation are devices that serve any of the following medical purposes: (i) diagnosis, prevention, monitoring, treatment or alleviation of disease; (ii) diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap (iii) investigation, replacement or modification of the anatomy or of a physiological process or (iv) control of conception.

[61] ENISA, 'Security and Resilience in eHealth Infrastructures and Services' (ENISA 2015) <https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services> accessed 18 December 2018

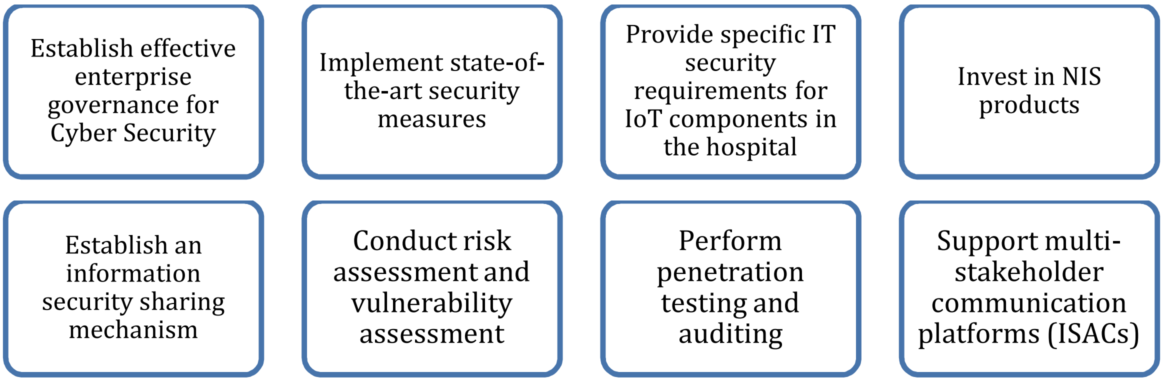
- Relevant good practices that have been deployed in the MS for eHealth security

5.2.2.3 Cyber Security and resilience for Smart Hospitals – ENISA Guidance

ENISA also published another, much more practical, report on 24 November 2016 entitled "Cyber Security and resilience for Smart Hospitals". Such report proposes key recommendations for hospital information security executives and industry to enhance the level of information security in Smart Hospitals.

This particular study focuses on IoT components supporting healthcare organisations in the context Smart Hospital ecosystems. Based on the analysis of documents and empirical data, and the detailed examination of attack scenarios found to be particularly relevant for smart hospitals, this document identifies mitigation techniques and good practices.[62]

As part of the key recommendation, ENISA is of the opinion that hospitals should do the following:



Establish effective enterprise governance for Cyber Security

Implement state-of-the-art security measures

Provide specific IT security requirements for IoT components in the hospital

Invest in NIS products

Establish an information security sharing mechanism

Conduct risk assessment and vulnerability assessment

Perform penetration testing and auditing

Support multi-stakeholder communication platforms (ISACs)

5.2.2.4 ISO Standards

As already mentioned above, the International Organisation for Standardisation (ISO) provides standards on information security risks, management and controls.

Some of those standards are specific to the health sector:

- ISO 27799:2016 on "Health informatics – Information security management in health using ISO/IEC 27002" provides guidelines for designing health sector specific information management systems[63] (replacing ISO 27799:2008 Health informatics - Information security management in health using ISO/IEC 27002)

- ISO 13485:2003 on "Medical devices – Quality management systems – Requirements for regulatory purposes"

- ISO 80001-1:2010 on "Application of risk management for IT networks incorporating medical devices"

[62] ENISA, 'Cyber Security and resilience for Smart Hospitals' (ENISA 2016) <https://www.enisa.europa.eu/publications/Cyber Security-and-resilience-for-smart-hospitals> accessed 18 December 2018

[63] ENISA is making reference to such standards in its mapping of the security requirements for operators of essential services.

5.2.2.5 US-driven instruments and guidance

The United States have been very active in the field of Cyber Security in the health sector, and to which ENISA is making reference (notably in its guidance its mapping of the security requirements for operators of essential services).

Such rules are based on the U.S. Health Insurance Portability and Accountability Act, known as the HIPAA. The "HIPAA Security Rule"[64] are currently the most commonly applicable standards across the healthcare sector and the U.S. Department of Health & Human Services (the "HHS") has notably published a Security Risk Assessment Too, the HIPAA Security Rule Toolkit, and the Guidance on Risk Analysis requirements under the Security Rule.

In addition to the above, the following instruments published in the U.S. can be of particular relevance to an organisation active in the specific health sector:

- ETSI eHealth Standard TR 102 764 eHEALTH; Architecture; Analysis of user service models, technologies and applications supporting eHealth

- Digital Imaging and Communications in Medicine (DICOM)

- NIST SP 800-66 An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Guide

5.3 Smart Shipping Management Pilot

As mentioned above, ships increasingly employ systems that rely on digitisation and automation. The growing use of disruptive technologies, such as big data, artificial intelligence and the 'Internet of things', comes with a surge in the volume of information processed in and transmitted between shipping systems. Thus, vessels but also shipping infrastructure may be exposed to Cyber Attacks or other vulnerabilities. A robust approach to maritime Cyber Risk management has therefore become indispensable.

The (cyber-)security legal and regulatory requirements relevant to the shipping industry are governed by, on the one hand, general security-related legal instruments, which are sometimes explicitly declared applicable to the shipping industry, and on the other hand, concrete security requirements and recommendations emitted by agencies, such as the International Maritime Organisation, and industry consortia.

Any (cyber-)security training should, to a certain extent depending on the target audience, take into account such legal requirements and recommendations. The present Section intends to give an illustrative overview of some of the instruments relevant to the shipping industry and the Smart Shipping Management Pilot.

5.3.1 General security and breach-related requirements

5.3.1.1 GDPR

As discussed in sub-Section 4.2.1.1 above, the GDPR applies to the processing of personal data in the context of the activities of an organisation established within the EU, or to the processing of personal data of individuals in the EU where such processing relates to the offering of goods or services to those individuals or the monitoring of their behaviour within the EU. As such,

[64] U.S. Department of Health & Human Services, 'The Security Rule' (HHS.gov, 12 May 2017) <https://www.hhs.gov/hipaa/for-professionals/security/index.html> accessed 18 December 2018

the GDPR has no sectorial approach, in the sense that it may apply horizontally and without distinction to organisations across different sectors and industries.

Therefore, in the event and to the extent the Smart Shipping Management Pilot processes personal data, it will be required to comply with the security and breach-related requirements imposed by the GDPR, which have been dealt with in sub-Section 4.2.1.1 above.

5.3.1.2 NIS Directive

Further information on the requirements of the NIS Directive has been given in sub-Section 4.2.1.2 above and will be made available in Deliverable D8.10.

It is however important to note in the context of the Smart Shipping Management Pilot that Annex II of the NIS Directive explicitly lists the following types of entities as potential "operators of essential services" to which the requirements of the NIS Directive would apply:

- Inland, sea and coastal passenger and freight water transport companies[65], not including the individual vessels operated by those companies;

- Managing bodies of ports[66], including their port facilities[67], and entities operating works and equipment contained within ports; and

- Operators of vessel traffic services.[68]

In light of the information currently available, it is however unlikely that the Smart Shipping Management Pilot would be qualified as an operator of essential services under the NIS Directive.

5.3.1.3 European Critical Infrastructures Directive

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection[69] (the "**European Critical Infrastructures Directive**") establishes a procedure for Member States to identify and designate European Critical Infrastructures ("**ECI**") on their respective territories.

A critical infrastructure is defined as "*an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions*", whereas an ECI is defined as a "*critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States*."

[65] As defined for maritime transport in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p. 6).
[66] As defined in point (1) of Article 3 of Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (OJ L 310, 25.11.2005, p. 28).
[67] As defined in point (11) of Article 2 of Regulation (EC) No 725/2004.
[68] As defined in point (o) of Article 3 of Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (OJ L 208, 5.8.2002, p. 10).
[69] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345, 23.12.2008, p. 75–82.

The Directive has a sectoral scope, applying only to the energy and transport sectors. Its Annex I presents a list of the relevant ECI sectors, which includes "ocean and short-sea shipping and ports" under the transport category. It is however up to the Member State concerned to determine whether a national critical infrastructure qualifies as an ECI.

5.3.2 Sector-specific security and breach-related requirements

5.3.2.1 IMO Guidelines on Maritime Cyber Risk Management

On 5 July 2017, the International Maritime Organisation (the "**IMO**") issued circular MSC-FAL.1/Circ.3 entitled "Guidelines on Maritime Cyber Risk Management".[70]

The Guidelines are targeted at all organisations in the shipping industry and aim to provide "*high-level recommendations on maritime Cyber Risk management to safeguard shipping from current and emerging Cyber Threats and vulnerabilities*".

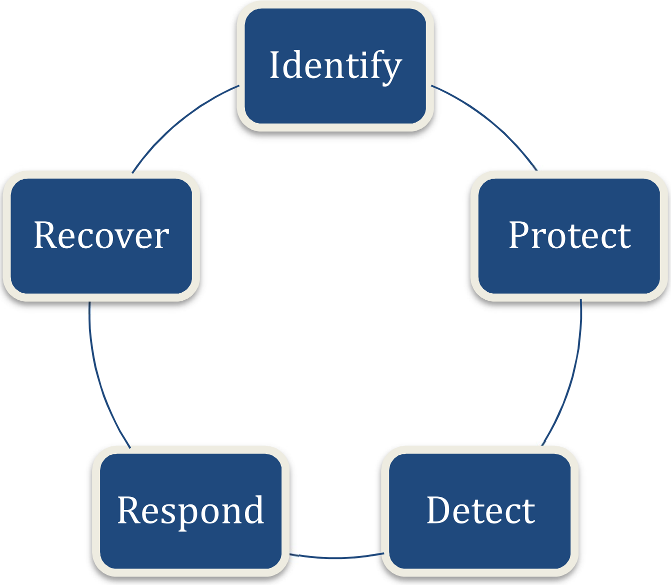
In this context, the Guidelines provide the following definitions:

- **Maritime Cyber Risk**: a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised

- **Cyber Risk management**: the process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders

According to the Guidelines, effective maritime Cyber Risk management can be achieved through a comprehensive assessment of the organisation's current Cyber Risk management and the performance of a gap analysis in respect of the organisation's desired Cyber Risk management. To this end, the five following functional elements should be concurrently and continuously integrated into the organisation's risk management framework:

[70] International Maritime Organisation, Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3), 5 July 2017, <http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf#search=maritime%20cyber%20risk>



Identify:

- Define Cyber Risk management roles and responsibilities
- Identify systems, assets, data and capabilities that may pose risk

Protect:

- Implement risk control processes and measures
- Implement contingency planning

Detect: Develop activities necessary to detect cyber events in a timely manner

Respond: Develop activities and plans to restore systems necessary for shipping operations

Recover: Identify measures to back-up and restore Cyber Systems necessary for shipping operations

The Guidelines further refer, in a non-exhaustive manner, to the following additional relevant guidance:

- The Guidelines on Cyber Security On-board Ships (see below)
- ISO/IEC 27001 standard on information technology – Security Techniques – Information security management systems – Requirements
- United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cyber Security (the NIST Framework)

5.3.2.2 IMO Resolution on Maritime Cyber Risk Management in Safety Management Systems

On 16 June 2017, the Maritime Safety Committee of the IMO adopted Resolution MSC.428(98) on "Maritime Cyber Risk Management in Safety Management Systems".[71]

The Resolution makes reference to the recommendations of the IMO Guidelines on Maritime Cyber Risk Management, which at that point in time had already been approved by the Facilitation Committee and the Maritime Safety Committee of the IMO.

[71] International Maritime Organisation, Resolution MSC.428(98) – Maritime Cyber Risk Management in Safety Management Systems, adopted on 16 June 2017, <http://www.imo.org/en/OurWork/Security/WestAfrica/Documents/Resolution%20MSC.428(98)%20-%20Maritime%20Cyber%20Risk%20Management%20in%20Safety%20Management%20Systems.pdf#search=maritime%20cyber%20risk>

According to the Resolution, an approved safety management system should take into account Cyber Risk management. This statement entails that Cyber Risk management comes within the scope of the International Safety Management (**ISM**) Code, which provides an international standard for the safe management and operation of ships at sea. The objective of safety management systems is to provide a safe working environment by establishing appropriate safe practices and procedures based on an assessment of all identified risks to the ship, on-board personnel and the environment. In the context of ship operations, Cyber Incidents are anticipated to result in physical effects and potential safety and/or pollution incidents. This means that organisations need to assess risks arising from the use of IT and OT on-board ships and establish appropriate safeguards against Cyber Incidents.

The Resolution thus encourages administrations to ensure that Cyber Risks are appropriately addressed in safety management systems no later than the first annual verification of the Company's Document of Compliance (i.e. a document issued to a company that complies with the requirements of the ISM Code) after 1 January 2021. It however acknowledges that certain safeguards may need to be put in place in order to guarantee the confidentiality of certain Cyber Risk management aspects.

Company plans and procedures for Cyber Risk management should be complementary to the existing security and safety risk management requirements contained in the ISM Code and the International Ship and Port Facility Security Code (**ISPS**) Code, which contains minimum security arrangements for ships, ports and government agencies. In accordance with chapter 8 of the ISPS Code, the ship is obliged to conduct a security assessment, which should include all operations that are important to protect. The assessment should address radio and telecommunications systems, including computer systems and networks (part B, paragraph 8.3 of the ISPS Code). This calls for controlling and monitoring "the ship to shore" path of the Internet connection, which is important owing to the fast adoption of sophisticated and digitalised on-board OT systems that in many cases have not been designed to be cyber resilient.

5.3.2.3 The Guidelines on Cyber Security On-board Ships (version 3)

The "Guidelines on Cyber Security On-board Ships" produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL[72] have been created as a guidance document addressed to ship owners and operators covering the necessary procedures and actions to preserve the security of Cyber Systems in their companies and on-board their ships.

The Guidelines are aligned with the IMO Resolution on Maritime Cyber Risk Management in Safety Management Systems and provide recommendations on maritime Cyber Risk management, both from a Cyber Security and cyber safety perspective.

It notably sets out the following Cyber Risk management approach for Cyber Security on-board ships:

[72] The Guidelines on Cyber Security On-board Ships (version 3), produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL, <https://www.bimco.org/products/publications/free/Cyber Security>

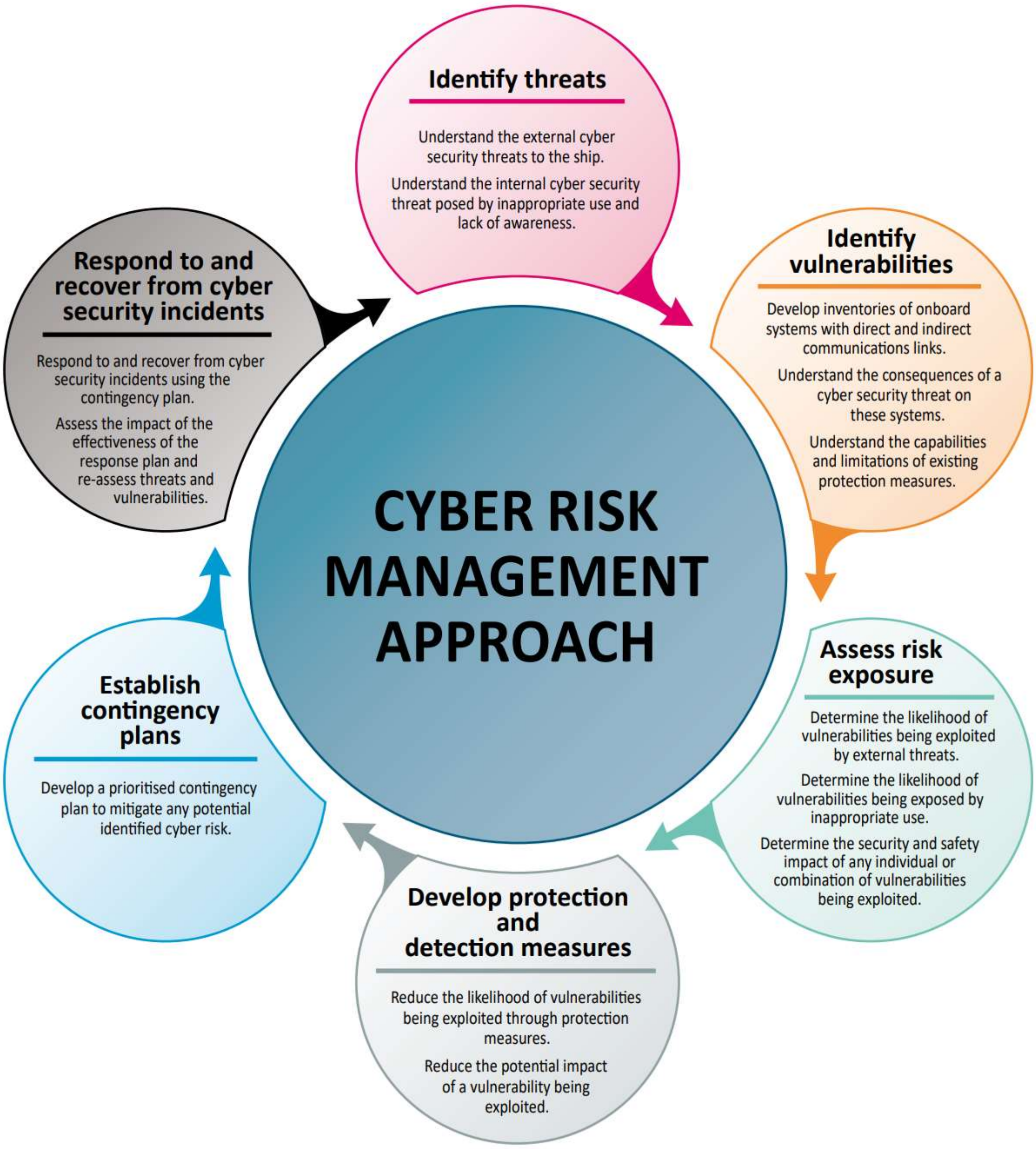

Identify threats
Understand the external cyber security threats to the ship.
Understand the internal cyber security threat posed by inappropriate use and lack of awareness.
Identify vulnerabilities
Develop inventories of onboard systems with direct and indirect communications links.
Understand the consequences of a cyber security threat on these systems.
Understand the capabilities and limitations of existing protection measures.
Assess risk exposure
Determine the likelihood of vulnerabilities being exploited by external threats.
Determine the likelihood of vulnerabilities being exposed by inappropriate use.
Determine the security and safety impact of any individual or combination of vulnerabilities being exploited.
Develop protection and detection measures
Reduce the likelihood of vulnerabilities being exploited through protection measures.
Reduce the potential impact of a vulnerability being exploited.
Establish contingency plans
Develop a prioritised contingency plan to mitigate any potential identified cyber risk.
Respond to and recover from cyber security incidents
Respond to and recover from cyber security incidents using the contingency plan.
Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.
CYBER RISK MANAGEMENT APPROACH

Figure 12. Cyber Risk management approach as set out in the Guidelines on Cyber Security On-board Ships

It shall be noted that the Guidelines contain a final chapter (chapter 7) on how to respond to and recover from Cyber Security incidents, without however covering incident notification requirements.

5.3.2.4 Further (cyber-)security guidance

Further guidance relevant for the shipping industry includes:

- European Network and Information Security Agency (ENISA), Analysis of Cyber Security Aspects in the Maritime Sector (November 2011)[73]

- The Institution of Engineering and Technology, Code of Practice - Cyber Security for Ports and Port Systems (16 August 2016)[74]

[73] https://www.enisa.europa.eu/publications/Cyber Security-aspects-in-the-maritime-sector-1

[74] https://www.gov.uk/government/publications/ports-and-port-systems-Cyber Security-code-of-practice

- The Institution of Engineering and Technology, Code of Practice – Cyber Security for Ships (13 September 2017)[75]
- American Bureau of Shipping, Guidance Notes on the Application of Cyber Security Principles to Marine and Offshore Operations – ABS CyberSafety™ Volume 1 (September 2016)[76]

- American Bureau of Shipping, Guide for Cyber Security Implementation for the Marine and Offshore Industries – ABS CyberSafety™ Volume 2 (September 2016, updated 15 June 2018)[77]

- American Bureau of Shipping, Guidance Notes on Data Integrity for Marine and Offshore Operations – ABS CyberSafety™ Volume 3 (September 2016)[78]

- The Danish Defence Intelligence Service's Centre for Cyber Security, Threat Assessment - The Cyber Threat against the maritime sector (March 2017)[79]

- Republic of the Marshall Islands, Marine Guideline No. 2-11-16: Maritime Cyber Risk Management (April 2018)[80]

[75] https://www.gov.uk/government/publications/ship-security-Cyber Security-code-of-practice

[76] https://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/250_cybersafetyV1/CyberSafety_V1_Cyber Security_GN_e.pdf

[77] https://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/251_cybersafetyV2/CyberSafety-V2-Cyber Security-Guide-June18.pdf

[78] https://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/252_cybersafetyV3/CyberSafety_V3_Data_Integrity_GN_e.pdf

[79] https://fe-ddis.dk/cfcs/cfcsdocuments/the_cyber_threat_to_the_maritime_sector_march.pdf

[80] https://www.register-iri.com/wp-content/uploads/MG-2-11-16.pdf

6 Evaluation Criteria and KPI's definition

Key Performance Indicators (KPIs) and evaluation criteria will be employed to determine to what degree THREAT ARREST achieved its purpose. Both are identified and described in the proposal under section 1.1.2, but supplementary KPIs or modifications of existing ones may arise whilst the evaluation framework is developed during Task 7.1. In subsection 6.1, table 6, we illustrate THREAT ARREST's objective and their current corresponding KPIs. While in subsection 6.2, we briefly explain the key targets of the evaluation.

6.1 KPI's

Table 6. Objectives and Key Performance Indicators (KPIs)

Objectives	KPIs
Objective 1: *To develop the means for specifying Cyber Security threat training and preparation models and programmes to drive the realization of the training process*	**[KPI-1.1]** Delivery of a language enabling the specification of CTTP models, covering (a) the cyber system components and cyber threats covered by a CTTP programme; (b) the ways of simulating components of a Cyber System and the Cyber Attacks against it; (c) the components of the system that may be emulated and the ways of emulating them; (d) the real system operational events that should be monitored and analyzed in order to assess the operational security status of a Cyber System in real time; (e) the actions that stakeholders are expected to take against Cyber Attacks (e.g., preparedness, incident detection and analysis, real time incident response, and post incident response) and the tools that may be used for this purpose. (Task3.1).
	[KPI-1.2] Delivery of a tool enabling the specification of CTTP models (*Task3.2*).
	[KPI-1.3] Delivery of a tool enabling the adaptation of CTTP models and programmes (*Task3.3*).
	[KPI-1.4] The language and tools to be developed should enable the specification of CTTP models and programmes as required for the pilots and by the KPIs [KPI-7.1], [KPI-7.2], [KPI-7.3], [KPI-7.4] and [KPI-7.6] (see *WP7*).
Objective 2: *To develop emulation capabilities enabling the creation of virtual cyber system components, subjecting them to Cyber Attacks for training purposes, and enabling trainees to take appropriate response actions and hands on experience against these Cyber Attacks.*	**[KPI-2.1]** Delivery of mechanisms enabling the emulation of all key types of software and physical components commonly found in a Cyber System, including web servers, data base servers, security servers, event busses, operating systems, trusted platform modules, and network components. (*Task2.1*)
	[KPI-2.2] For each type of emulated component the developed mechanisms will support defend and attack actions by individual users and user groups and the logging of these actions (Task2.1).
	[KPI-2.3] The developed capabilities will be able to simulate cyber systems with full accuracy with respect to the cyber threats and attacks targeted by a CTTP programme (Task2.3).
	[KPI-2.4] Delivery of mechanisms enabling the monitoring of the emulated component's status and the actions performed on them by the trainees (Task2.2).
	[KPI-2.5] Delivery mechanisms automating the process of creating and interlinking the emulated components (*Task2.3*).

	[KPI-2.6] The developed emulation capabilities will improve average trainee skills in avoiding the relevant Cyber Attacks by at least 80% (see *WP7*).
Objective 3: *To develop multi-layer simulation capabilities enabling the realistic simulation of cyber systems, their usage and security attacks launched on them, through synthetic events at all layers in the implementation stack of these systems and their components reflecting realistic system conditions.*	**[KPI-3.1]** Delivery of mechanisms to support (a) static and dynamic statistical profiling of events, (b) generation of synthetic event logs, (c) the propagation of the synthetic events through the connected simulated components of the cyber system, and (d) the simulation of the operations of individual cyber system components (*Task5.1*).
	[KPI-3.2] The developed mechanisms will enable the simulation of all key types of software and physical components commonly found in a Cyber System, including web servers, data base servers, security servers, event busses, operating systems, trusted platform modules, and network components (*Task5.3).*
	[KPI-3.3] The developed mechanisms will enable the generation of synthetic event logs for all the main different types of events that may be typically found in a Cyber System, including operating system and cyber system component operation calls, network traffic (*Task5.2).*
	[KPI-3.4] The developed capabilities will be able to simulate cyber systems with full accuracy with respect to the cyber threats and attacks targeted by a CTTP programme (*Task5.3).*
	[KPI-3.5] The developed simulation capabilities will improve average trainee skills in avoiding the relevant Cyber Attacks by at least 80% (see *WP7*).
Objective 4: *To develop Cyber Security training based on serious games and enable trainees to get engaged in cyberdefence, elicit threats and learn about attacks.*	**[KPI-4.1]** Delivery of serious games to cover all social engineering attacks identified in the pilot and the main types of such attacks across different systems (*Task4.2*).
	[KPI-4.2] The developed serious games will improve average trainee skills in avoiding social engineering based Cyber Attacks by at least 80% (see *WP7*).
Objective 5: *To develop key capabilities for the effective delivery of CTTP programmes, i.e., the visualization of the operation and state of cyber systems and the emergence and effects of attacks against them; assessing trainee performance in CTTP programmes and adapting them depending on it; and assessing the overall effectiveness of a CTTP programme and evolving it accordingly.*	**[KPI-5.1]** Delivery of visualization tools covering the state of the real and the simulated/emulated cyber system; the attacks upon them; the effects of user actions; comparative performance measures (e.g., individual trainee performance vs group performance, performance over different time periods, performance for different threats/attacks) and the capability to zoom in and out on parts of the system and the events related to them (*Task4.1*).
	[KPI-5.2] Delivery of mechanisms to support evaluation of trainee performance based on subjective information obtained through questionnaires and objective information through the monitoring and analysis of trainee actions and at all layers of the evaluation framework advocated in Sect. 1.3.3 of the proposal (*Task4.3*).
	[KPI-5.3] Delivery of mechanisms to support the adaptation of CTTP programmes for individual trainees (*Task4.5*).
	[KPI-5.4] Delivery of mechanisms to support the evolution of CTTP programmes following evaluation across trainee groups (*Task4.4*).

Objective 6: *To align training and simulation with the continuous security assurance of real operational cyber systems, by integrating the capabilities developed under Objectives 1-5 into a common platform together with security assurance assessment capabilities.*	**[KPI-6.1]** Deliver two separate (i.e., an initial and a final) prototypes of *the THREAT-ARREST* platform (*Task6.1-6.2*).
	[KPI-6.2] The prototypes will offer integrated assurance/monitoring, emulation, simulation, serious gaming, training and visualization capabilities (*Task6.1*).
	[KPI-6.3] The final prototype of the platform will be delivered at Technology Readiness Level (TRL) 7, i.e., as a prototype system demonstrated in a real operational environment (*Task6.1-6.3*).
Objective 7: *To display the use of the THREAT-ARREST framework for effective training against Cyber Attacks in the domains of smart energy, healthcare and transport (shipping), using real operational cyber systems within these domains as pilots and, through them, evaluate and validate the framework.*	**[KPI-7.1]** Provide effective CTTP models and CTTP programmes for all known attacks and standardized security assurance profiles of all the three pilot systems of the project (*Task1.1, Task3.2*).
	[KPI-7.2] The developed CTTP models and programmes will cover threats against: (i) key security property types (i.e., confidentiality (C), integrity (I), availability (AV) and authentication (AU)), (ii) key data states (i.e., data-in-transit, data at-rest and data-in-processing), and (iii) physical and software components of cyber systems (*Task1.1, Task3.2*).
	[KPI-7.3] The developed CTTP models and programmes will target and cover different types of trainees, including software engineers, security experts, system administrators, end users, security auditors2, and where applicable chief information-officers and Chief-Security-Officers. They also cover public and private system users (*Task7.1,Task3.2*).
	[KPI-7.4] The developed CTTP models and programmes will cover different types of action including preparedness, detection and analysis, security incident response and post security incident response (*Task1.1, Task3.2*).
	[KPI-7.5] The user-based evaluation of the framework with regards to the support that it offers in developing new CTTP programmes and providing adequate response in attacks that have led to organisational level emergency situations will be no less than 90% of the maximum user grade that may be given to the relevant criteria (see *WP7*).
	[KPI-7.6] The CTTP programmes and the framework itself will be fully aligned with obligations stemming from applicable legal frameworks. The KPIs **[KPI-2.3]** and **[KPI-3.4]** defined under Objective 2 and Objective 3 are also relevant to this objective (*Task8.5*).
Objective 8: *To ensure the uptake, commercialization, and the delivery of innovation of project outcomes by developing an ecosystem around the THREAT-ARREST framework.*	**[KPI-8.1]** Events for security solutions developers, resulting in at least 5 such developers, who are not members of the *THREAT-ARREST* consortium, providing CTTP models for their solutions using the *THREAT-ARREST* framework (*Task8.1*).
	[KPI-8.2] Events for cyber system developers, resulting in at least 5 such developers, who are not members of the *THREAT-ARREST* consortium providing new components for it (*Task8.1*).
	[KPI-8.3] Achieve the project's dissemination targets as defined in Table 6 of Sect. 2.2.2 as well as in Table 8 of Sect. 2.2.6 of the proposal (*Task8.3*).

	[KPI-8.4] Align CTTP programmes with security training programmes to provide effective training for related examinations. The targeted security training programmes are ISACA – CISA/CISM [169][170], ISC$_2$ – CISSP [166], CSA – Cloud Security [167], SANS – GIAC [168] (*Task3.4*).
	[KPI-8.5] Achieve affiliated programmes status for at least one of the following security training programmes: ISACA – CISA/CISM, ISC$_2$ – CISSP, CSA – Cloud Security, SANS – GIAC (*Task8.4*).

6.2 Evaluation Criteria

The evaluation will focus on validating the framework from (a) technical, (b) business and (c) legal perspectives. The overarching target of the evaluation will to assess the ability of the framework to increase the effectiveness of response against Cyber Attacks. This should cover all different types of responses, [5][6] i.e., preparedness, incident detection and analysis, real time incident response, and post incident response. Other key evaluation criteria under (a) will include the comprehensiveness and realism of simulations (i.e., coverage of attacks and system usage conditions), the usability and effectiveness of the framework for a variety of trainee profiles. Evaluation under (b) will include an assessment of the ability of the framework to define new CTTP models and amend existing CTTP models for existing Cyber Attacks in a cost-effective manner, as well as providing effective training for responding adequately to attacks that have led to organisational level emergency situations. Evaluation under (c) will include an assessment of the alignment of the CTTP programmes delivered by the framework with obligations stemming from applicable legal frameworks.

7 Concluding Remarks: Pilot's Requirements table

The three complementary fields of the THREAT-ARREST pilots have different needs and deficiencies in terms of security awareness. In the case of the Smart Energy System, the lack of secured protocols makes it easy to gain access and control of a smart home. Consumers are rarely aware of the security and privacy concerns of IoT devices and often opt for ease-of-use instead of security. In the healthcare industry there are many types of threats and potential attackers that the personnel tasked with defending an organisation needs to be aware of. Companies and ships, in the Smart Shipping use-case, may fall victims of an attack either explicitly or as a consequence of a more generic breach attempt, using tools and techniques that are widely available. The on-board and shore-side staff needs to be trained in order to be able to identify a potential compromisation attempt.

As the training platform, that is the goal of this project, is starting to be developed in this initial phase, it is important to first lay out its requirements. The pilots' training and security requirements identified and analyzed here, in addition to the system requirements of the tools that will be used in the platform, are essential in building the THREAT-ARREST architecture in the next step of the combined consortium effort.

The pilot Cyber Systems have been selected due to the fact that they involve: (a) different and heterogeneous types of system components and devices; (b) different security and privacy cyber- threats and requirements; and (c) different types of actors that need to receive training. These pilots from three diverse fields of industry will play a pivotal role in the overall adoption of the outcome of the project, as they will prove the global applicability of the platform.

This deliverable – along with D1.2 – forms the basis on top of which the initial version of the reference architecture for the THREAT-ARREST platform will be developed.

A consolidated overview of requirements for each pilot in reference is displayed below:

Table 7. Consolidated table of requirements of three pilots

Req-Id	Description	Req Level (MUST/SHOULD)	Indicative Use-Case scenario
Energy_R_01	IoT Authentication and Authorization	Must	Authentication and authorization are essential parts of basic security processes and are sorely needed in the Internet of Things (IoT). The emergence of edge and fog computing creates new opportunities for security and trust management in the IoT. Efficient and scalable trust management for the IoT based on locally centralized, globally distributed trust management using an open source infrastructure with local authentication and

			authorization entities to be deployed on edge devices.
Energy_R_02	Emerging Technologies for IoT Security	Must	Emerging Technologies Spearheading The IoT Security. For example: 1. **Blockchain** is already being considered as a panacea for all security and accountability related issues faced by multiple industries. The inherent security features of Blockchain makes it an ideal choice for implementing various security measures in IoT. From data security, to managing authorizations and device identification, Blockchain is being imagined as the middleware security layer for IoT systems. Many of these ideas are in the research phase, and some initial implementations exist. **2. Software Defined Networking (SDN)** With the threat of large scale DDoS attacks looming over the Internet and orchestrated through a huge army of compromised IoT devices, there is a lot of research going on in the areas of early detection of such attacks. SDN can possibly offer a solution to this. The SDN controllers which administer a network domain can communicate with

			SDNi, a set of specifications that enable Inter SDN controller communication. By exchanging information through SDNi, the neighbor SDN controllers can gauge some early warnings signs about an imminent DDoS attacks targeting computers in their neighborhood. This can immensely help network administrators to take corrective actions in time to mitigate the further propagation of attacks. **3. AI & Big Data** A big data repository of such metrics can be leveraged to run machine learning models for conducting periodic audit of networks for possible IoT security breaches. We have seen Google and other online services employing such measures to authenticate user access to their services. If you remember Google asking you for your location, or confirming your account through an OTP, then you know whats happening behind the scenes. There is big data and AI at play which checks for any anomaly in user access, such as

			location change, too frequent logins or even periodic checks. Something in similar lines needs to be done for IoT devices as well.
Energy_R_03	Possibilities for Hackers on IoT devices	Must	Examples and real cases of attacks in the residential Sector. Having the ability to heat up your house before you get home or use your phone to control when the coffee pot turns on really isn't a technology to be dismissive of. Using your voice to tell your TV what to play makes people feel as though they're living in the future. These rewards lead people to continue buying the new IoT device, even though their security might be on the line. So, going into the years ahead, the question cannot be about making people value their security over convenience. Instead, it should be about educating IoT professionals to do more to make their IoT devices secure and transparent with how they manage customer's information.
Energy_R_04	Lightweight cryptography for the Internet of things	Should	This topic must give an overview of the state-of-the-art technology and standardiza-tion status of lightweight cryptography, which can be implemented efficiently in constrained devices. This technology enables secure and efficient communication between networked smart objects.
Energy_R_05	Analyzing the Risks	Should	This topic combines knowledge of Security Risk Management with existing practice in securing in IoT into a framework, which aim

			is to cover vulnerabilities in IoT systems in order to protect users' data. We propose an initial comprehensive reference model to management security risks to the information and data assets managed and controlled in the IoT systems. Based on the domain model for the information systems security risk management, we explore how the vulnerabilities and their countermeasures defined in the distributed energy context.
Energy_R_06	Elliptic curve cryptography (ECC) asymmetric algorithm	Must	The elliptic curve cryptography (ECC) asymmetric algorithm is widely promoted to developers for new Internet of Things (IoT) advancements. Constraints in IoT include limitations to computational resources such as the bare minimum processor speed and memory needed as such devices are typically designed for low power consumption. Challenges include the need to reengineer things such as identity management, device and user registration, and cryptography to suit IoT needs.
Energy_R_07	WiFi Vulnerabilities and security measures	Must	Common protocol vulnerabilities and ways to secure and maintain confidentiality, integrity,

			and availability over this protocol
Energy_R_08	ZigBee Vulnerabilities and security measures	Must	Common protocol vulnerabilities and ways to secure and maintain confidentiality, integrity, and availability over this protocol
Energy_R_09	MQTT Vulnerabilities and security measures	Must	Common protocol vulnerabilities and ways to secure and maintain confidentiality, integrity, and availability over this protocol
Energy_R_10	CoAP Vulnerabilities and security measures	Must	Common protocol vulnerabilities and ways to secure and maintain confidentiality, integrity, and availability over this protocol
Health_R_01	Train user to identify risk related to email authenticity	Must	The user will receive email from known contacts with malicious code and link; assess the behavior of the user
Health_R_02	Train user on basic Internet navigation and update procedures	Must	The user will be faced with possible tool and update download from suspicious and known website; assess the compliance of the user on security policies
Health_R_03	Train administrator on basic database management and protection procedure	Must	The administrator will face attacks of SQL injection and attempt to assess to central and distributed databases
Health_R_04	Raise awareness on the threat of external computers and equipment joining the network	Should	The administrator need to apply suitable countermeasures in case of attacks coming from external computers and equipment that are added to the network; the administrator should react in case the common security policies does not protect in full the architecture.
Health_R_05 (from Shipping_R_05)	Train designated IT security personnel of the Agency for risks related to poor software and data security practices where no anti-virus checks or	Should	The users will face frequent system crashes to assess their awareness on system malfunction along with mitigation actions

	authenticity verifications are performed		that users should take and route cause analysis that users should perform as countermeasure
Health_R_06 (from Shipping_R_07)	Train user on identifying Cyber Risks in relation to the physical presence of non-Agency personnel	Should	System infrastructure will be attacked by compromising equipment, software or supporting services being delivered to the Agency or Hospitals by third-party providers, e.g. where third-party technicians are left to work on equipment without supervision
Health_R_07 (from Shipping_R_06)	Train user over safeguarding information, passwords and digital certificates	Must	Trigger a scenario where unexpected password changes or authorized users being locked out of a system
Shipping_R_01	Train user to identify risks related to emails and how to behave in a safe manner	Must	Phishing attacks where a user of e.g. supplier department is called via email to click on a link to a malicious site to reach a candidate supplier in order to request quotations
Shipping_R_02	Train user to identify risks related to Internet usage, including social media, chat forums and cloud-based file storage where data movement is less controlled and monitored	Should	Social Engineering attacking while e.g. crew on-board is interacting with social media through WiFi when vessel is at terminal
Shipping_R_03	Train user to identify risks related to the use of own devices (these devices may be missing security patches and controls, such as anti-virus, and may transfer the risk to the environment to which they are connected)	Should	Trigger a scenario where a malware is infecting company's network at shore due to connection of a network component (e.g. user workstation) with suspicious uncertified devices (user mobile).
Shipping_R_04	Train user to identify risks related to installing and	Must	Trigger a scenario where an update of ECDIS navigation system is performed with an

	maintaining software on company hardware using infected hardware (removable media) or software (infected package)		uncertified USB. False Objects on digital nautical charts will be displayed along the route and user will be assessed over identifying any anomaly on navigational information and the mitigation action that should take.
Shipping_R_05	Train designated IT security personnel of the company for risks related to poor software and data security practices where no anti-virus checks or authenticity verifications are performed	Should	Release frequent system crashes to assess user awareness on system malfunction along with mitigation actions that user should take and route cause analysis that user should perform
Shipping_R_06	Train user over safeguarding information, passwords and digital certificates	Must	Trigger a scenario where unexpected password changes or authorised users being locked out of a system
Shipping_R_07	Train user on identifying Cyber Risks in relation to the physical presence of non-company personnel,	Should	Attacking office or ship by compromising equipment, software or supporting services being delivered to the office or ship by third-party providers. e.g, where thirdparty technicians are left to work on equipment without supervision
Shipping_R_08	Raise awareness of the consequences or impact of Cyber Incidents to the safety and operations of the ship and the readiness or knowledge of user to mitigate risks by evaluating the user on following standard controls over risk in case of a Cyber Threat or attack	Must	Assessor component activated in every platform training scenario to checkout real time the set of actions trainee takes against standard procedures in case of a Cyber Attack.

All -R_01	Train user on general and specific security-related legal framework and to identify violation of legal security requirements in case of a breach	Must	Any breach of security may point at a violation by the organisation of general or specific security requirements imposed upon it and would therefore require the organisation's personnel to identify and remediate such violations in order for it to improve compliance with its security-related obligations
All -R_02	Train user on statutory and non-statutory breach notification requirements	Must	Any breach of security may entail a breach notification obligation internally within the organisation or externally and would therefore require the organisation's personnel to assess the breach and identify the existence of any such statutory or non-statutory notification requirements.

8 References

1. American Bureau of Shipping (2016). Guidance notes on the application of cybersecurity principles to marine and offshore operations. ABS CyberSafety Volume 1. Available at: https://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/250_cybersafetyV1/CyberSafety_V1_Cybersecurity_GN_e.pdf [Accessed 18 Dec. 2018].
2. American Bureau of Shipping (2018). Cybersecurity implementation for the marine and offshore industries. ABS CyberSafety Volume 2. Available at: https://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/251_cybersafetyV2/CyberSafety-V2-Cybersecurity-Guide-June18.pdf [Accessed 18 Dec. 2018].
3. American Bureau of Shipping (2016). Data integrity for marine and offshore operations. ABS CyberSafety Volume 3. Available at: https://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/252_cybersafetyV3/CyberSafety_V3_Data_Integrity_GN_e.pdf [Accessed 18 Dec. 2018].
4. Article 29 Data Protection Working Party (2016). Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002)58/EC). Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf [Accessed 18 Dec. 2018].
5. Article 29 Data Protection Working Party (2018). Guidelines on Personal data breach notification under Regulation 2016/679. Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 [Accessed 18 Dec. 2018].
6. Brennan, D, 2013. New rules on breach notification by telcos and ISPs - clarity at last?. PDP Journals, Volume 6, issue 5, 4. Available at: https://www.algoodbody.com/media/DataProtectionArticle_DaviniaBrennnan1.pdf [Accessed 18 Dec. 2018].
7. BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL (2017). The Guidelines On Cyber Security On-board Ships Version 3. Available at: https://www.bimco.org/products/publications/free/cyber-security [Accessed 18 Dec. 2018].
8. Cesena, M., et al. 2017. SHIELD Technology Demonstrators. CRC Press, Book for Measurable and Composable Security, Privacy, and Dependability for Cyberphysical Systems, pp. 381-434.
9. Centre for Cyber Security (2017). The cyber threat against the maritime sector. Available at: https://fe-ddis.dk/cfcs/cfcsdocuments/the_cyber_threat_to_the_maritime_sector_march.pdf [Accessed 18 Dec. 2018].
10. Commission Implementing Regulation (EU) 2018/151 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact [2018] OJ L 26/48.
11. Commission Regulation (EU) 611/2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications [2013] OJ L 173/2.
12. Council Directive (EC) 2008/114 of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [2008] OJ 345/75.

13. Data Protection Authority (2017). Big Data Rapport. Available at: https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Rapport_Big_Data_2017.pdf [Accessed 18 Dec. 2018].

14. De Muynck, J. and Portesi, S. (2016) Strategies for incident response and cyber crisis cooperation, Enisa. doi: 10.2824/967546.

15. DNV GL Maritime Advisory and GARD (2018). Cyber Security Awareness in the Maritime Industry. Available at: http://www.gard.no/Content/25634225/Cyber%20Security_Presentation%20(ID%201418279).pdf [Accessed 18 Dec. 2018].

16. DNV GL Maritime Advisory (2016). Cyber Security Resilience Management for Ships and Mobile Offshore Units in Operation. Available at http://www.gard.no/Content/21865536/DNVGL-RP-0496.pdf [Accessed 18 Dec. 2018].

17. DNV GL Maritime Advisory (2017). Cyber Security and Shipping. Available at: http://cd502fa18faf34612009-6be874ed8f905033bd346f731eef6b8c.r48.cf1.rackcdn.com/Patrick%20Rossi.pdf [Accessed 18 Dec. 2018].

18. Directive (EC) 1999/5 of the European Parliament and of the Council on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity [1995] OJ L 91/10.

19. Directive (EC) 2002/21 of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services [2002] OJ L 108/33.

20. Directive (EC) 2002/58 of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector [2005] OJ L 201/37.

21. Directive (EC) 2002/59 of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC [2002] OJ 208/10.

22. Directive (EC) 2005/65 of the European Parliament and of the Council of 26 October 2005 on enhancing port security [2005] OJ 310/28.

23. Directive (EC) 2005/89 of the European Parliament and Council of 18 January 2006 concerning measures to safeguard security of electricity supply and infrastructure investments [2005] OJ 33/22.

24. Directive (EC) 2009/72 of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC [2009] OJ L211/55.

25. Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1.

26. ENISA (2011). Cyber Security Aspects in the Maritime Sector. Available at: https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1 [Accessed 18 Dec. 2018].

27. ENISA (2015). Security and Resilience in eHealth Infrastructures and Services. Available at: https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services [Accessed 18 Dec. 2018].

28. ENISA (2016). Cyber Security and resilience for Smart Hospitals. Available at: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals [Accessed 18 Dec. 2018].

29. ENISA (2016). Smart Hospitals Security and Resilience for Smart Health Service and Infrastructures. Available at: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals [Accessed 18 Dec. 2018].

30. ENISA (2017). Incident Notification for DSPs in the Context of the NIS Directive, A Comprehensive Guideline on How to Implement Incident Notification for Digital Service Providers in the Context of the NIS Directive. Available at: https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive [Accessed 19 Dec. 2018].

31. European Commission (2018). Summary report on the public consultation on the Evaluation and Review of the ePrivacy Directive. Available at: https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-evaluation-and-review-eprivacy-directive [Accessed 18 Dec. 2018].

32. European Commission (2017). Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (2017/0003(COD).

33. Hatzivasilis, G., et al., 2016. Software Security, Privacy and Dependability: Metrics and Measurement. IEEE Software, IEEE, vol. 33, issue 4, pp. 46-54.

34. Hatzivasilis, G., et al., 2018. The Industrial Internet of Things as an enabler for a Circular Economy Hy-LP: A novel IIoT Protocol, evaluated on a Wind Park's SDN/NFV-enabled 5G Industrial Network. Computer Communications – Special Issue on Energy-aware Design for Sustainable 5G Networks, Elsevier, vol. 119, pp. 127-137.

35. Healthcare Industry Cyber Security Task Force (2017). Report on Improving Cyber Security in the Healthcare Industry. Available at: https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf [Accessed 18 Dec. 2018].

36. Institution of Engineering and Technology (2016). Code of Practice: Cyber Security for Ports and Port Systems. Available at: https://www.gov.uk/government/publications/ports-and-port-systems-cyber-security-code-of-practice [Accessed 18 Dec. 2018].

37. Institution of Engineering and Technology (2017). Code of Practice: Cyber Security for Ships. Available at https://www.gov.uk/government/publications/ship-security-cyber-security-code-of-practice [Accessed 18 Dec. 2018].

38. International Maritime Organisation (2017). Guidelines on Maritime Cyber Risk Management. Available at: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf [Accessed 18 Dec. 2018].

39. International Maritime Organisation (2017). Maritime Cyber Risk Management in Safety Management Systems. Available at: http://www.imo.org/en/OurWork/Security/WestAfrica/Documents/Resolution%20MSC.428(98)%20-%20Maritime%20Cyber%20Risk%20Management%20in%20Safety%20Management%20Systems.pdf#search=maritime%20cyber%20risk [Accessed 18 Dec. 2018].

40. National Institute for Standards and Technology (2012). Computer Security Incident Handling Guide. Available at: https://citadel-information.com/wp-content/uploads/2012/08/nist-sp800-61-draft-computer-security-incident-handling-guide-2012.pdf [Accessed 18 Dec. 2018].

41. National Institute of Standard and Technology (2018). Cyber Security Framework. Available at https://www.nist.gov/cyberframework [Accessed 18 Dec. 2018].

42. National Institute of Standards and Technology (2018). Framework for Improving Critical Infrastructure Cyber Security. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [Accessed 18 Dec. 2018].

43. NIS Cooperation Group (2018). Reference Document on Incident Notification for Operators of Essential Services, Circumstances of Notification. Available at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53644 [Accessed 18 Dec. 2018].

44. NIS Cooperation Group (2018). Guidelines on Notification of Operators of Essential Services Incidents. Formats and Procedures. Available at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53677 [Accessed 17 December 2018].

45. Manifavas, C., et al., 2014. DSAPE – Dynamic Security Awareness Program Evaluation. Human Aspects of Information Security, Privacy and Trust (HCI International 2014), 22-27 June, 2014, Creta Maris, Heraklion, Crete, Greece, Springer, LNCS, vol. 8533, pp. 258-269.

46. Maritime Administrator of the Republic of the Marshall Islands (2018). Maritime Cyber Risk Management. Available at: https://www.register-iri.com/wp-content/uploads/MG-2-11-16.pdf [Accessed 18 Dec. 2018].

47. McKee, D. (2018). 80 to 0 in Under 5 Seconds: Falsifying a Medical Patient's Vitals. Available at: https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/80-to-0-in-under-5-seconds-falsifying-a-medical-patients-vitals/ [Accessed 18 Dec. 2018].

48. Regione Puglia (2008). DGR 01/08/2008 n. 1500 "Istituzione Registro Regionale dei Tumori. Protocollo d'Intesa e Comitato Tecnico Scientifico". Available at: http://www.regione.puglia.it/documents/10192/5132977/N153_01_10_2008.pdf/7a71f9ac-4834-431f-9d6f-b95a525248ad [Accessed 18 Dec. 2018].

49. Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1

50. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC [2017] OJ 117/1.

51. Regulation (EC) 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security [2004] OJ L129/6.

52. U.S. Department of Health & Human Services (2017). The Security Rule. Available at: https://www.hhs.gov/hipaa/for-professionals/security/index.html [Accessed 18 Dec. 2018].

53. U.S. Government (1996) Health Insurance Portability And Accountability Act. Available at: https://www.govinfo.gov/content/pkg/PLAW-104publ191/html/PLAW-104publ191.htm [Accessed 18 Dec. 2018].

54. AVAST (2018), "AVAST Research on 16/08/2018", Available at: https://press.avast.com/avast-research-finds-at-least-32000-smart-homes-and-businesses-at-risk-of-leaking-data

55. Kolias C, Kambourakis G, Stavrou A, Voas J (2017), "DDoS in the IoT: Mirai and Other Botnets", Volume: 50 , Issue: 7 , 2017, Available At: https://ieeexplore.ieee.org/document/7971869/authors#authors