Speech: Protecting the maritime industry from cyber attacks

Good afternoon ladies and gentlemen.

It's a real pleasure to be here.

This is my first experience of London International Shipping Week.

I've heard so many positive things about it.

So I'm delighted to be able to join you today (13 September 2017).

And to talk about an issue which has such profound significance in our modern world.

Cyber security is an increasing concern for many industries across the global economy.

And that certainly includes maritime.

Anything that threatens the reliability and performance of a shipping sector that carries 95% of our trade has to be taken seriously.

In some areas, maritime continues to rely on legacy systems using old software and aging operational technology.

There is also growing dependence on information systems with the development of new technologies – such as autonomous or partially-autonomous vessels.

This has the potential to make the industry more vulnerable to cyber attacks.

And the implications of such vulnerabilities could be highly damaging.

Poor cyber security undermines customer confidence and industry reputation, and could potentially result in severe financial losses or penalties, and litigation affecting the companies involved.

The disruption caused by a cyber attack – or a compromised system – could be significant too.

Just consider what a compromised ship system could trigger:

- physical harm to the system or the shipboard personnel or cargo – potentially endangering lives or the loss of the ship
- the loss of sensitive information, including commercially sensitive or personal data
- criminal activity, including kidnap, piracy, fraud, theft of cargo, or imposition of ransomware

Even if the problem is on a much smaller scale, it could play havoc with an industry that requires order and reliability to operate efficiently.

Cyber security is not just about preventing hackers gaining access to systems and information.

It’s also about protecting digital assets and information, ensuring business continuity, and making sure the maritime industry is resilient to outside threats.

That means not only keeping ship systems safe from physical attack, but also ensuring that supporting systems are robust.

So that in the event of an incident, appropriate practices and technologies are in place to limit any damage.

There is also the need for personnel security – guarding against the possible threat from insiders, either shore or shipboard-based.

Ship owners and operators need to understand cyber security and promote awareness of the subject to their staff and business partners.

In recent years the government has demonstrated how seriously we take the cyber security threat.

The 2015 National Security Strategy reaffirmed cyber as a Tier One risk to UK interests.

We have dedicated cyber security teams in a range of departments working with the industry, manufacturers, international partners and academia.

This includes officials within the Department for Transport.

We have a team that works with shipping industry partners, port operators and vessels traffic services (VTS) organisations.

And have cyber security teams working with other transport sectors – such as aviation, rail, and connected and autonomous vehicles.

Our aims are to:

- understand the cyber threat and the vulnerabilities for the transport sector
- mitigate cyber risks and take appropriate action to protect key assets
- respond to cyber incidents effectively and ensure that lessons are learnt

and promote cultural change, raise awareness and build cyber capability.

The government also established the National Cyber Security Centre in 2016 – again to work with the industry on this increasingly complex subject.

You will be hearing from the security centre in just a few moments.

All this preparation is time – and money – well spent.

Because in recent months, we have seen some high profile cyber attacks hit various part of the economy.

Including maritime.

The NotPetya cyber attack in June (2017) hit many different organisations across the globe including some in the shipping sector.

It showed that the industry is vulnerable to these type of attacks.

And we may encounter many more in the years to come.

So we want to support the maritime sector to help you manage your cyber security risks.

That’s why I want to tell you about the Department for Transport’s new Cyber Security code of practice for ships.

You should have some hard copies with you, but it is also available on gov.uk from today.

This guidance is aimed at ship operators, ship owners and crew members.

Businesses of all sizes.

And it will help you:

- develop a cyber security assessment and plan
- devise the most appropriate mitigation measures
- ensure you have the correct structures, roles, responsibilities and processes in place

and manage security breaches and incidents.

It also highlights the key national and international standards and regulations that should be reviewed and followed.

The Department for Transport commissioned the Institution of Engineering and Technology (IET) to produce the code of practice.

It has also received input from experts at the Maritime Coastguard Agency, Maritime Accident and Investigation Branch, the MoD’s Defence Science and Technology Laboratory, and the National Cyber Security Centre.

The guidance will complement the work being done by the International Maritime Organisation (IMO) to raise awareness of cyber threats and vulnerabilities.

This code of practice explains why it is essential that cyber security be considered as part of a holistic approach throughout a ship’s lifecycle.

As well as setting out the potential impact if threats are ignored.

The code of practice is intended to be used as an integral part of a risk management system to ensure that cyber security is delivered cost effectively as part of mainstream business.

This latest code of practice follows on from last year’s publication of the well-received Cyber security code of practice for ports and port systems, which is also available on GOV.UK.

The ports code of practice was also written by IET, so both guidance documents are consistent in their approach.

We hope you find it of value, and encourage you to consider all the advice.

We will continue to work with you all and seek to ensure that the UK’s transport sector remains safe, secure and resilient in the face of cyber threats, and able to thrive in an increasingly interconnected, digital world.

Thank you.