News story: Emergency Services Show 2017

Air, Rail and Marine Accident Investigation Branches at the Emergency Services Show, 20-21 September

Are you one of the first emergency services on the scene of an air, marine or rail accident? Perhaps you manage a control room for one of the emergency services. If so, you'll want to visit our stand at the Emergency Services Show. We are the AAIB, MAIB and RAIB – the three independent branches of the Department for Transport that investigate air, marine and rail accidents.

To help prevent similar accidents from happening again, our evidence gathering starts from the point of notification through search and rescue stages to forensic examination of the site. At the Emergency Services Show, our staff will be on hand to tell you everything you need to know so that if you're at an accident site, you can help preserve evidence that can provide us with vital clues to establish the cause.

Transport accidents pose some serious difficulties to the emergency services. Ballistic recovery systems in small aircraft, confined spaces on ships, 100s of tonnes of dangerous goods inside derailed freight rail wagons. Would you know how to approach evidence preservation in these environments?

Visit us at the Show to learn about all of this and more.

Emergency Services Show website

News story: 4th Annual Meeting of the Global Islamic Finance and Investment Group

Senior policy makers from around the world met in London yesterday (12 September 2017) to discuss cross-border cooperation to further boost the global Islamic finance industry at the 4th annual meeting of the Global Islamic Finance and Investment Group (GIFIG).

Islamic finance, or Sharia-compliant finance, has seen remarkable growth over the last decade. The value of the industry more than doubled between 2008 and 2015, and the sector is full of potential to grow further still, providing greater choice and giving people the financial products that can meet their

values.

The annual meetings of GIFIG form a key part of the UK's commitment to support the development of the industry globally, and ensure that London, which is already home to the largest Islamic finance market outside the Muslim world, retains its top position.

The meeting was co-chaired by Minister of State for Asia and the Pacific, Mark Field, and the Economic Secretary to the Treasury, Stephen Barclay who said:

> The UK is recognised as the leading Western centre for Islamic finance, and I want us to play a big part in the future of the sector. London is the most globally connected financial centre, providing a nexus of expertise in financial, professional and supporting services. And with our strong links with other outward looking economies, including those with significant Muslim populations, we are ideally placed to play a central role.
>
> I am delighted to welcome representatives from so many countries interested in the development of Islamic finance to London to discuss how we make sure that people from all walks of life have access to appropriate finance.

This year's meeting of GIFIG looked at areas where countries with an interest in Islamic finance can work better together to support the development of the industry. Discussions also covered responses to the industry's on-going market and regulatory challenges and synergies between Islamic and other areas of finance.

The UK has a track record of supporting Islamic finance. UK firms have been involved in Islamic finance since the 1980s and the UK has been at the forefront of key developments in Europe ever since. The UK today is one of the few jurisdictions worldwide that accommodates Islamic finance within a single and secular regulatory framework. There are now over 100,000 Islamic finance retail customers in the UK, benefiting from Sharia-compliant current accounts, home finance, savings, investment and other products.

Press release: Have you checked your heating oil tank?

With an autumnal nip in the air, the Environment Agency is urging anyone with a domestic heating oil tank to check their tank is in a good state of repair before getting heating oil delivered for the winter.

Leaks and spills from a domestic heating tank can be difficult and expensive to clean up; leaked oil can end up in groundwater supplies and drains, many of which lead directly into rivers, streams, lakes and even garden ponds.

If oil does get into drains it could pollute watercourses; harming livestock, wildlife and plants. Our vital drinking water can also come from the same surface and groundwater supplies so protection is important.

Oil is poisonous to fish, other wildlife and smothers plants – just two litres of oil could seriously pollute the volume of fresh water needed to fill an Olympic-size swimming pool.

Steve Brown from the Environment Agency said:

> Heating oil can cause serious problems if it gets into the water environment.
>
> The clean-up costs could be tens of thousands of pounds; and these costs fall to the owner of the leaking tank. These costs are not always covered by household insurance policies. A serious case of land contamination from a leaking oil tank could also severely affect the value of property in the area.
>
> This is why it's vital that oil is only ever stored in tanks that are in good condition. Both the tank and its pipe work should be regularly inspected and people should never buy more oil than they can safely store.
>
> If anyone does find a spill, please contact us straight away so that we can reduce the impact on the environment.

To report an oil spill people should contact the Environment Agency's 24-hour incident hotline on 0800 80 70 60.

Press release: Hull people smuggler jailed

Arnoldes Jocys, 19, pleaded guilty yesterday (12 September) at the start of his scheduled four day trial at Hull Crown Court and was sentenced immediately to 27 months' imprisonment. He had been charged with facilitating a breach of the UK's immigration laws.

Jocys had been stopped by Border Force officers at the Port of Hull on the morning of 16 May. He had arrived on an overnight ferry from Rotterdam and was driving a Mercedes Sprinter van.

When questioned by officers, Jocys said he was delivery driver and that he was carrying a mixed load of vodka, beer, cigarettes, furniture and barbecues.

Mark Robinson, Border Force Assistant Director with the Humber Command, said:

> Jocys was nervous when he was being spoken to and when the rear of the van was searched it became obvious why. As officers unloaded the contents, they found, hiding behind a sofa, two Chinese men. The cargo area had been filled floor to ceiling with goods. It was clear the Chinese men could not have found their way into the vehicle without assistance.

Jocys, of no fixed UK address, was arrested and the case was passed to Immigration Enforcement's Criminal and Financial Investigation (CFI) Team. In interview, the two Chinese men said they had been placed into the van in Belgium, although they could not say by whom. They were returned to Belgium later the same day (16 May).

Subsequent forensic examination found that the rear and side doors of the van had been fitted with a new locking system which meant they could only be opened with a key from the outside.

Mike Reed, CFI Inspector, said:

> This evidence supported the prosecution case that the two illegal migrants could not have got into the rear of the van without Jocys' knowledge.
>
> This was a shameless attempt to bypass the UK's immigration controls that was prevented thanks to the expertise of my colleagues in Border Force. With the evidence they provided, alongside our own investigations, we have been able to bring a would-be people smuggler to justice.
>
> I hope that this case sends a clear message to anyone else tempted to get involved in criminality of this type – you will be caught and brought before the courts.

Anyone with information about suspected immigration abuse can contact Crimestoppers on 0800 555 111 anonymously or visit http://www.crimestoppers-uk.org.

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.